Tiago Filipe
Santos Silvério

# Implementação Fotónica de Funções Fisicamente Não Clonáveis

# Photonic Implementation of Physically Unclonable Functions

Tiago Filipe
Santos Silvério

# Implementação Fotónica de Funções Fisicamente Não Clonáveis

# Photonic Implementation of Physically Unclonable Functions

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Física, realizada sob a orientação científica da Doutora Maria Rute de Amorim e Sá Ferreira André, Professora Associada com Agregação do Departamento de Física da Universidade de Aveiro e do Doutor Paulo Sérgio de Brito André, Professor Catedrático do Departamento de Engenharia Electrotécnica e de Computadores do Instituto Superior Técnico da Universidade de Lisboa.

This work was developed within the scope of the project CICECO-Aveiro Institute of Materials, FCT Ref. UID/CTM/50011/2021), Instituto de Telecomunicações (FCT Ref. UID/EEA/50008/2021), WINLEDs (POCI-01-0145-FEDER-030351) financed by national funds through the FCT/MEC and when appropriate co-financed by FEDER under the PT2020 Partnership through European Regional Development Fund (ERDF) in the frame of Operational Competitiveness and Internationalization Programme (POCI).

**o júri / the jury**

| | |
|---|---|
| presidente / president | **Prof. Doutora Margarida Maria Resende Vieira Facão**<br>Professora Auxiliar da Universidade de Aveiro |
| arguente / examiner | **Prof. Doutor Orlando José dos Reis Frazão**<br>Professor Assistente convidado da Universidade do Porto |
| orientador / supervisor | **Prof. Doutora Maria Rute de Amorim e Sá Ferreira André**<br>Professora Associada c/ Agregação da Universidade de Aveiro |
| coorientador / co-supervisor | **Prof. Doutor Paulo Sérgio de Brito André**<br>Professor Catedrático do Instituto Superior Técnico de Lisboa. |

**Agradecimentos / Acknowledgements**

Em primeiro lugar, gostaria de agradecer à Professora Rute Ferreira e ao Professor Paulo André pelas oportunidades que me proporcionaram e pela confiança que depositaram em mim. Todo o seu apoio e ensinamentos foram determinantes no meu desenvolvimento académico e, em particular, no desenvolvimento deste trabalho.

A todos os membros do grupo Phantom-G, agradeço o ambiente, companheirismo e auxílio que me proporcionam desde o primeiro dia. Em particular, agradeço à Lília Dias pelo seu contributo, disponibilidade e imensa colaboração em todos os aspetos técnicos deste trabalho.

Aos meus pais e às minhas irmãs, agradeço a excelente educação e apoio que sempre me deram. Apesar da distância, todos os dias mostram carinho, dedicação e compreensão em todos os aspetos da minha vida. Agradeço também ao meu irmão Pedro pela companhia, a confiança, os todos os incentivos que me deu para este trabalho e para a minha vida. Sem este apoio incondicional, nada disto seria possível.

Um especial agradecimento à Catarina, à Joana e à Mariana, pela amizade, apoio incondicional e paciência comigo. Não tenho como vos agradecer por toda a motivação e conselhos que me deram para este trabalho. Certamente que o meu percurso ficou e ficará marcado pela vossa presença.

Por fim, um enorme obrigado à Ana pelo constante suporte, carinho e tranquilidade que me tem dado longo destes anos. Qualquer tarefa se torna muito mais fácil quando se tem alguém tão inspiradora e entusiasmante como tu.

**Palavras-chave**

Funções óticas físicamente não clonáveis, sistemas criptográficos, padrões de espalhamento ótico coerente, internet das coisas, anti-falsificação, híbrido orgânico-inorgânico.

**Resumo**

Nesta dissertação pretende-se estudar e desenvolver Funções Fisicamente Não Clonáveis, dispositivos caracterizados por terem variações aleatórias intrínsecas, sendo, portanto, elegíveis para sistemas de alta segurança devido à sua impossibilidade de clonagem, unicidade e aleatoriedade. Com a rápida expansão de tecnologias como a Internet das Coisas e as preocupações com produtos falsificados, os sistemas criptográficos seguros e resilientes são altamente requisitados. Além disso, o desenvolvimento de ecossistemas digitais e de aplicações móveis para transações comerciais requerem algoritmos rápidos e seguros de geração de chaves criptográficas. A natureza estatística das imagens baseadas no *speckle* cria uma oportunidade para o aparecimento desses geradores de chaves criptográficas.

No contexto deste trabalho, três dispositivos diferentes foram implementados como funções fisicamente não clonáveis, nomeadamente, papel vegetal, fibra óptica de plástico e um híbrido orgânico-inorgânico. Estes objetos foram submetidos a um estímulo de luz coerente na região espectral visível e produziram um padrão de *speckle* o qual foi utilizado para recuperar a chave criptográfica associada a cada um dos materiais. A metodologia implementada neste trabalho incorpora a Transformada Discreta de Cosseno, o que possibilita a criação de um sistema criptográfico de 128 bits caracterizado por ser semi-compacto e de baixo custo. O protocolo de autenticação exigiu a análise de múltiplas respostas de diferentes *Physically Unclonable Functions* (PUFs), o que permitiu estabelecer um nível de limite de decisão ótimo de forma a maximizar a robustez e minimizar a probabilidade de erro por parte do sistema. O sistema de encriptação de 128 bits atingiu valores de probabilidade de erro abaixo do limite de deteção, $10^{-12}$, para todas as amostras, mostrando o seu potencial como gerador de chaves criptográficas.

**Keywords**

Optical physically unclonable functions, cryptographic systems, optical coherent speckle pattern, internet of things, anticounterfeiting, organic-inorganic hybrids.

**Abstract**

This dissertation aimed to study and develop optical Physically Unclonable Functions, which are physical devices characterized by having random intrinsic variations, thus being eligible towards high security systems due to their unclonability, uniqueness and randomness. With the rapid expansion of technologies such as Internet of Things and the concerns around counterfeited goods, secure and resilient cryptographic systems are in high demand. Moreover the development of digital ecosystems, mobile applications towards transactions now require fast and reliable algorithms to generate secure cryptographic keys. The statistical nature of speckle-based imaging creates an opportunity for these cryptographic key generators to arise.

In the scope of this work, three different tokens were implemented as physically unclonable devices: tracing paper, plastic optical fiber and an organic-inorganic hybrid. These objects were subjected to a visible light laser stimulus and produced a speckle pattern which was then used to retrieve the cryptographic key associated to each of the materials. The methodology deployed in this work features the use of a Discrete Cosine Transform to enable a low-cost and semi-compact 128-bit key encryption channel. Furthermore, the authentication protocol required the analysis of multiple responses from different samples, establishing an optimal decision threshold level that maximized the robustness and minimized the fallibility of the system. The attained 128-bit encryption system performed, across all the samples, bellow the error probability detection limit of $10^{-12}$, showing its potential as a cryptographic key generator.

# Contents

# List of Figures

# List of Tables

# Acronyms List

**CCD** Charge-Coupled Device

**CMOS** Complementary Metal–Oxide–Semiconductor

**CRP** Challenge-Response Pair

**DCT** Discrete Cosine Transform

**ECC** Error Correction Code

**FNR** False Negative Rate

**FPR** False Positive Rate

**HD** Hamming Distance

**IoT** Internet of Things

**PoE** Probability of Error

**PUF** Physically Unclonable Function

**RoI** Region of Interest

# CHAPTER 1

# Introduction

In this introductory chapter, the motivation for this work is presented as well as the objectives, state of the art, dissertation layout and contributions provided by this study.

## 1.1 Motivation

The Internet of Things (IoT) is a network of devices linked in real time which interact over a wired or wireless link with no human surveillance [1]. Such network has been proven to be fundamental in the development of smart cities and smart houses [2,3]. Due to its role in both present and future societies, IoT has been gathering increasingly attention by the scientific and general communities, being highlighted over the years [4, 5].

In a report published in 2020, Fortune Business Insights indicated that the global market for IoT is forecasted to reach $1.11 trillion by 2026 at a 24.7% compound annual growth rate [6]. Likewise, the International Data Corporation estimates that, by the year of 2025, 152 200 IoT devices will be connected every minute, which implies a forecast of nearly 80 billion devices by that year [7].

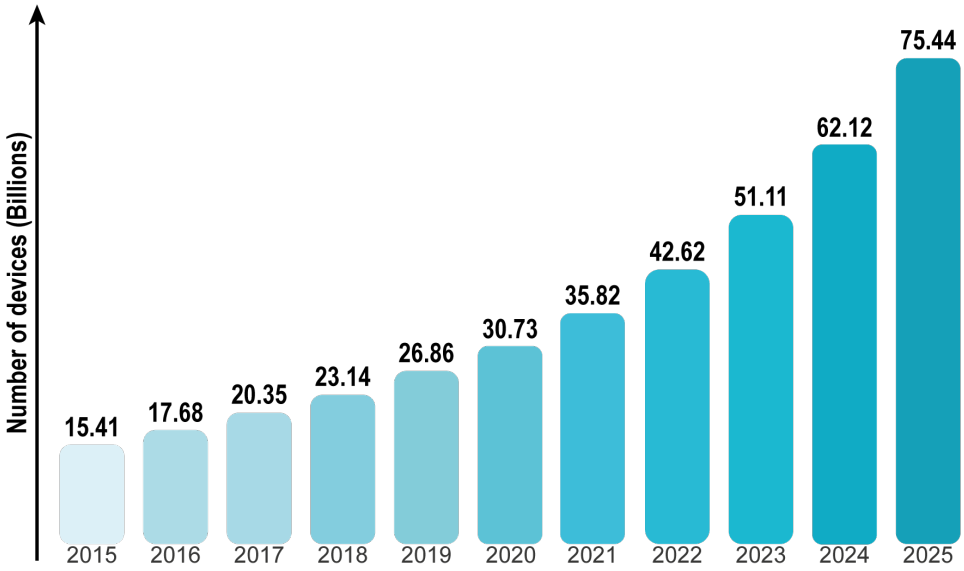


Figure 1.1: Surveyed (from 2015-2020) and estimated (2020 and onward) data for the number of IoT devices operating worldwide [7].

Moreover, a report performed by Netscout unveiled that 5 minutes is the average time that takes for a IoT device to be attacked once it accesses the internet and that 76% of the surveyed professionals believed that IoT left them at a greater risk of cyberattacks [8]. Evidently, the steady growth and development of such technologies will lead to more efficient networks. However, expanding such networks also represents a higher threat risk concerning the safety and security of these connections. Since potential security problems must be anticipated and act on before the network is fully expanded, these issues play an important role in pacing the technological development.

The aforementioned concerns are highlighted and supported by the fact that cyberattacks aiming IoT are spiking and becoming more relevant since they are an effective way to access a whole network only by hacking into a specific less-protected node in the network [9, 10]. As previously stated, although the IoT advantages are clear, they also present a huge risk, thus being imperative the implementation of measures to secure these systems from cyberattacks.

Another security concerning field is the counterfeiting of goods. The trading of goods is a global network with a large number of recipients in a variety of places with established connections, physical or otherwise. Despite the benefits of having a quick and easy access to these goods, motivated by technology, the trade of counterfeited proprieties is the second largest source of organized crime income, with illicit drug trade being number one [11]. It is estimated that, just in the year of 2020, the total value of exchanged counterfeiting goods reached over 1.82 trillion dollars [12]. In this value, it is included a variety of different types of counterfeiting goods, including apparel, currency, fuels, automotive components, pharmaceuticals and microelectronics [11]. Although, in most of these fields the items are secured by brand protection guidelines, the lower prices and stock abundance of the counterfeited goods lead to inevitable and wide-spread exchanges.

To tackle these security issues, this work features the Physically Unclonable Function (PUF). PUFs are real physical devices characterized by having a unique structure that is practically impossible to reproduce. These mechanisms provide an innovative and cheap alternative for authentication and remote key storage, i.e., without requiring a physical location to store the key, thus showing the high potential for this technology to be used in cryptographic systems, mainly, in unique key and random number generation [13]. Moreover, IoT networks rely heavily on the quality of random number generators and their storage proprieties, requiring the user to possess a unique key to access the network upon authentication-based protocols [14]. These conditions are fully achievable by using PUFs as a cryptographic key generator, which function both as secure key provider and remote access key storage.

In some cases, the counterfeited items pose immediate threat to human lives such as the counterfeiting of pharmaceuticals [15]. Hence, it is imperative to find solutions to guarantee the authenticity of medicine. To achieve a better authentication process of pharmaceuticals, one has to identify each unit with a non-reproducible and unique key. With that in consideration, and like in IoT authentication, PUFs can play an

important role by solving this issues with their ability to produce such unique and irreproducible keys, providing a safe authentication environment [1].

This dissertation addresses these security issues, relevant in many areas of modern technology, by using optical PUFs which rely on the coherent illumination of a dispersive token to produce unique and complex optical images for cryptographic key extraction [16]. Instead of using electronic PUFs, optical PUFs were chosen due to their higher security scores against targeted attacks and also higher unclonability and tamper resistance [17].

## 1.2 Objectives

The focus of this work is the optical implementation and characterization of PUF devices. As previously stated in section 1.1, these devices can play a crucial role in increasing the security amongst various areas such as IoT and product tagging. The solution proposed by this study is to use several different physical objects (tokens) as identifiers for optical PUF-based authentication. The technique to be applied for key extraction using the speckle image produced by each token is the type-II Discrete Cosine Transform (DCT). The tokens selected in the scope of this work are: tracing paper, a small segment of commercial plastic optical fiber and a monolith-shaped organic-inorganic hybrid.

Initially, an experimental system was designed to integrate all the optical components necessary to both produce and acquire high quality images of the output retrieved from each of the tokens. Since the responses of the tokens to the laser light excitation are dependent on the token position in relation to the rest of the system, custom optimized place holders for all the different tokens were considered. Furthermore, it is important that the tests to each of the PUF tokens are similar in order to determine if their structural differences yield different performance results and, in this case, their advantages and disadvantages were considered.

The imaging system chosen to acquire the speckle images, in order to produce high quality images, was optimized and, therefore, a series of test images were taken to ensure that the camera used is suited for this application.

The performance tests were divided in two distinct sections: authentication and security scores. The authentication scores are determined by comparing the different outputs of the tokens and, in this case, the normalized hamming distance will be used in order to distinguish the different devices. As for security purposes, several statistical tests were performed to determine the output randomness of each token along with the probability of error (PoE) tests applied to the authentication process.

## 1.3 State of the Art

Chaotic systems have been widely implemented in cryptographic systems over the past decades. The prediction difficulty in the outcome of physical chaotic systems creates the perfect environment to exploit these proprieties in robust authentication systems [18]. One of the first novelties in cryptographic systems, directly associated with PUFs, was introduced in 2001 [19]. In that work, many possible circuit realizations based on electronic PUFs were described and implemented in field programmable gate arrays to perform individual device authentication. The implementation of silicon-based PUFs took advantage of the intrinsic statistical variations on the delays of the devices and wires within the integrated circuit, to produce unique and unpredictable outputs, creating a manufacturer resistance PUF [19].

A year later, Pappu et. al suggested another approach, where, instead of PUF, the author described these devices as physical one-way functions [20]. However, rather than relying on the electrical proprieties of a device, in this case, the unpredictable system arises from the photonic implementation of the PUF. Hence, the study was based on a solitary optical waveguide providing insight about the usage of coherent radiation on an inhomogeneous microstructure to produce a speckle pattern on a screen, as shown in Figure 1.2.

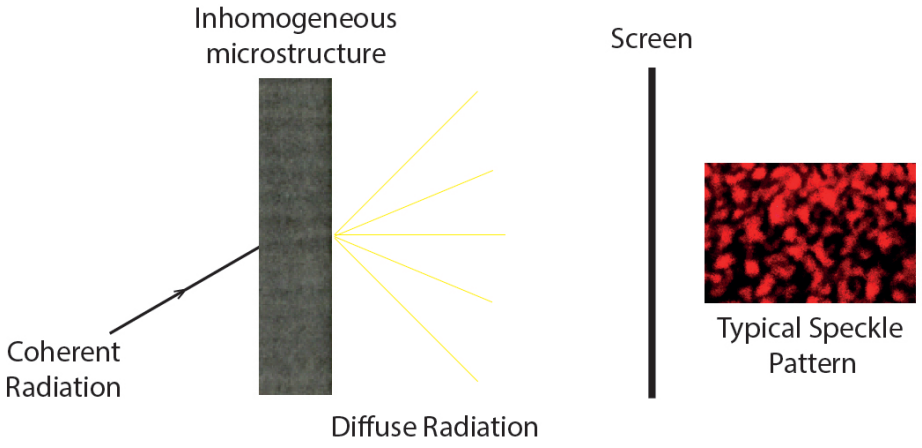


Figure 1.2: Illustration of the setup used to produce a speckle pattern based on the coherent illumination of an inhomogeneous microstructure.

Such prototype utilized the 3-dimensional microstructure, which has an underlying disordered formation, to produce an interference-based pattern, while having the coherent radiation as the probe. It was shown that the output of the interaction between the physical system and the probe can be used to robustly derive a unique tamper-resistant identifier at a very low cost per bit [20]. Although in this work, no security analysis was taken, based on the nature of the system, the prototype assumes a chaotic form, which reveals to be a cryptographic system in itself. Different authentication protocols were applied, including a one-time pad protocol, that illustrates the utility of

these hash functions on potential attacks of the authentication system considered. Additionally, the concept of fabrication complexity was introduced as a way of quantifying the difficulty of materially cloning physical systems with arbitrary internal states. As for the hash extraction technique, these systems were based on the Gabor Hash, using the Gabor filter for image frequency analysis, while deploying the fractional hamming distance as the metric for device distinction [17, 20].

Another alternative for optical PUF configuration based on a multimode optical waveguides was described by Mesaritakis et al. [13]. Similarly to [20], the hash extraction was made using the Gabor coefficients and, considering 1000 PUFs, a 256-bit encryption system was achieved. In this work, the main performance test consisted in comparing the curve profile of the histograms of intra hamming distance (intra-HD) and inter hamming distance (inter-HD), which compares the extracted keys from similar and different devices, respectively. Within this research landscape, the intra-HD/inter-HD technique is widely used to perform device authentication tests and, therefore, will also be reported in this dissertation. Additionally, subsequent to the hash extraction, an error correction code (ECC) was implemented, i.e., by allocating a certain amount of key bits, one can correct some of the errors that occurred during the extraction process [21]. However, the key redundancy is proportional to the number of bits allocated for ECC purposes and, thus, the authors assessed the performance of the system regarding the number of bits allocated for ECC [13]. Results shown in this work reflect that, with an ECC using 5 bits, the clonability probability associated with the PUF authentication process is $10^{-4}$. However, by only using an ECC with 5 bits, the robustness of the system is greatly compromised, yielding around 5%. To achieve maximum robustness, close to 100%, it is necessary to use an ECC of 40 bits which, however, indicates that there is a 100% probability of cloning, which greatly disqualifies the usage of such a high amount of ECC bits.

In [14], an IoT-oriented, PUF-based, 256-bit authentication system was described using the optical challenge of He-Ne laser that illuminates a 1.5 cm large core commercial plastic optical fiber. The novelty introduced by this article is that, prior to the interaction with the large-core plastic optical fiber, the intensity spatial profile of the laser beam is modulated using a liquid crystal display, as shown in Figure 1.3.

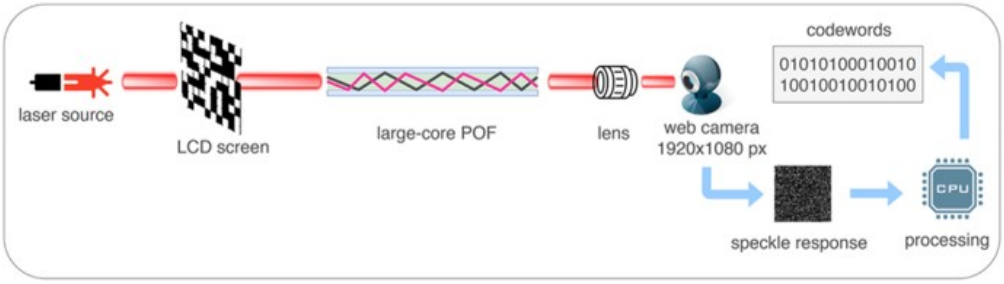


Figure 1.3: Representation of the experimental optical PUF system used in [14], with particular emphasis in the position of the liquid crystal display screen, which modifies the laser beam intensity spatial profile to achieve modulated optical challenges.

Using this configuration, 250 images were collected over 4 hours and the authors proceeded with the usual intra-HD/inter-HD analysis of the data acquired. The results pointed that this PUF system is robust while using an ECC of 30 allocated bits without greatly compromising the unpredictability of the system, which achieved a value of $10^{-5}$. Additionally, this article proposes the implementation of such system in an IoT network edge protection protocol, Figure 1.4.

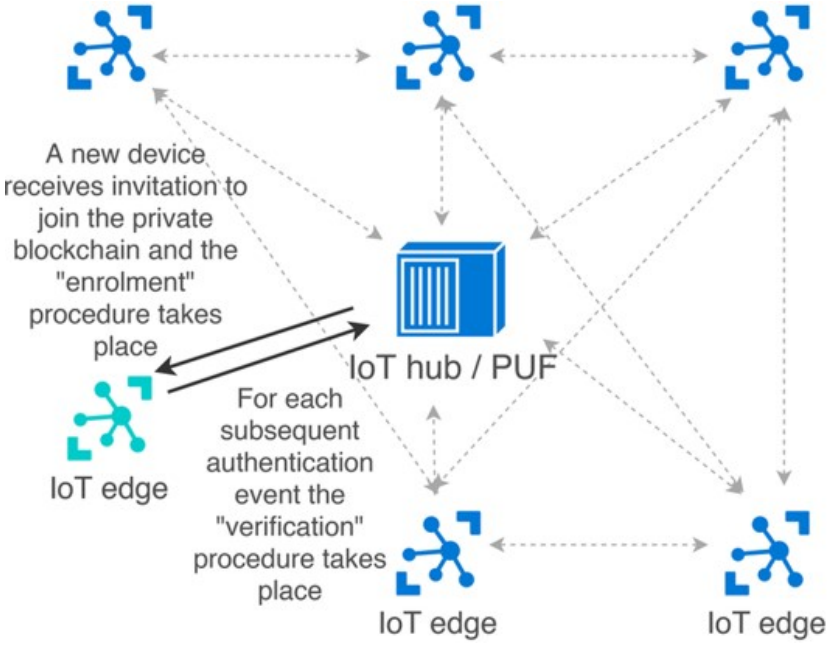


Figure 1.4: Schematics of an IoT network composed by several IoT edges, i.e. connected devices, and an IoT Hub characterized by performing the device authentication based on the CRP produced by the PUF device [14].

This schematic representation of the IoT network edge protection illustrates the uses that PUF can have inside IoT. In this case, if a device wishes to be authenticated and entering the IoT network, instead of retrieving the key from the IoT hub, it is the hub that generates such key, on demand, according to the challenge emitted by the user. This means that even if the IoT hub is compromised, each device is fully secure and their individual keys cannot be retrieved due to the one-way nature of the PUF challenge-response pairs (CRPs). Likewise, if an IoT edge is compromised and a malicious third-party gains access to their key, they will not be able to reverse engineer the process that originated that key, granting security to all of the other devices, including the IoT hub. These proprieties of PUF devices integrated in IoT networks with their respective authentication protocols are also described in-depth in [1], although with the implementation of a silicon-based electronic PUF device.

Another approach to optical authentication based on PUF devices was accomplished using the emission features of lanthanides, primarily utilizing this device as a cryptographic key generator in anticounterfeiting systems [15]. A physical key was made by producing a random pattern formed from taggants made from zeolite 5A (Linde Type

A), where the counterions ($Ca^{2+}$) have been exchanged by three different relevant lanthanide(III) ions. The authentication method deployed in this research included an emission-resolved imaging that allows to differentiate the different taggants using their unique emission spectra fingerprint. Additionally, a spectrometer allied with a filter-based detection, allowed the excitation-selection readout of each taggant which, when unknown to the public, adds an additional layer of security to the physical key. Following the targeted emission detection, a charge-coupled device (CCD) was used as the imaging device to record the pattern formed by the taggants, combining all of their contributions in a single image. From this work resulted a nominal encoding capacity of $6 \times 10^{104}$, which is more than relevant for anticounterfeiting and unique tagging purposes. Moreover, a false positive rate (FPR) of nearly $10^{-96}$ was achieved, which is well below the detection limit and one of the best results in the literature.

One of the reasons that electronic PUFs have been dominant over optical ones is their ability to be created as an integrated system that is notable due to their low-cost implementation and small size. In that regard, efforts are being made to find a solution to have integrated optical PUF systems, such as the one reported by Urban et al. [17]. A prototype of an integrated optical PUF that functions without moving components was accomplished, and its performance evaluated as well as its security. It was shown that these devices can be attacked by machine learning techniques if the employed scattering structure is linear, and if the raw interference images of the PUF are available to the adversary. With those considerations, a non-linear scattering structure was implemented within the integrated PUFs and 400 images were recorded and the Gabor coefficients were extracted, to extract the cryptographic key. The reported results yielded a 1.23% euclidean distance between the predicted response and the obtained response based on the 400 CRPs, which was considered a success in the authentication.

## 1.4 Dissertation Layout

This dissertation will be divided according to the following five chapters:

- **Introduction**, which is the current chapter, an overall view of the current state of the art for PUF devices, namely for optical PUFs, is presented, as well as the motivation for this work.

- **Fundamentals and Background**, that includes the theoretical concepts concerning optical sources and imaging technologies, along with the mathematical formulation applied to PUFs and the hashing process.

- **PUF Experimental Implementation**, which covers the experimental features are highlighted such as the description of the PUF tokens and the optical components chosen to integrate the system and their principal features.

- **Experimental Results** consisting of the experimental results regarding the performance of the optical PUFs and their security scores according to the present formulation.
- **Conclusion and Future Work**, which incorporates the conclusions of this work in addition to possible approaches and suggestions of corrections to be developed in the future.

# CHAPTER 2

# Fundamentals and Background

## 2.1 Optical Sources and Detectors

The production, enrollment and interrogation of PUF devices requires the use of specific components and concepts related to photonics. In this section, it will be described the principles of operation of coherent optical sources and imaging devices.

### 2.1.1 Laser

Producing speckle-based PUF devices requires radiation with very unique proprieties. To meet these requirements, the optical excitation source used in this work was the laser (light amplification by stimulated emission of radiation). Within the scope of this study, some of the laser beam proprieties are going to be studied due to their relevance in the systems performance.

The physical principles underlying the laser device were predicted by Einstein [22], applied in 1953 in a similar device called maser (microwave amplification by stimulated emission of radiation) [23], and then proved by Maiman [24], with the invention of the first ruby laser. The analysis of their physical structure can be made highlighting three major components: a pumping system, an active medium and a cavity [25]. Different arrangements and proprieties of these components are going to define the lasers optical output characteristics. A typical He-Ne gas laser layout and main components can be seen in Figure 2.1.

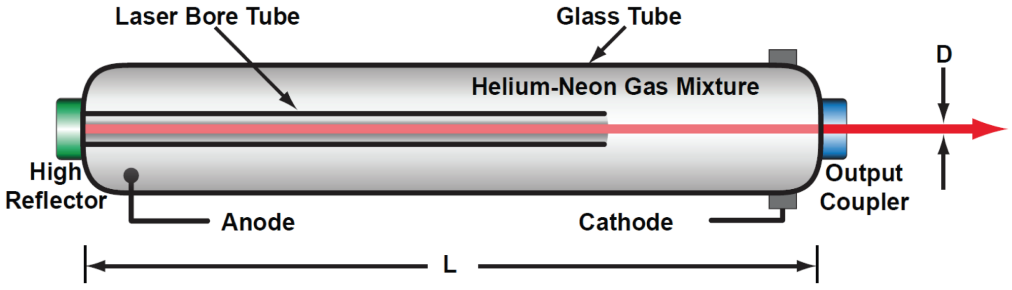


Figure 2.1: Illustration of the components of a He-Ne laser, namely, the cavity with an active medium (He-Ne mixture) and the couplers (high reflector and output mirrors). In this case, $D$ represents the beam width when exiting the device. Image adapted from [26].

Following the above-mentioned example of a He-Ne laser, the basic operation prin-

ciple of a laser can be explained considering the energy levels both of He and Ne, described in Figure 2.2. When a transition of a carrier occurs between two levels, either an absorption or an emission of a photon is involved, obeying to the energy conservation of the system. For this conservation to occur, the photon absorbed/emitted has to have the same energy as the difference in energy between the initial and final levels in the atom, $\Delta E$, which corresponds to a frequency of $\nu = \Delta E/h$, where $h$ is the Plank constant [27]. Although the absorption process requires a photon to stimulate the carrier transition, that is not entirely true for the emission process.

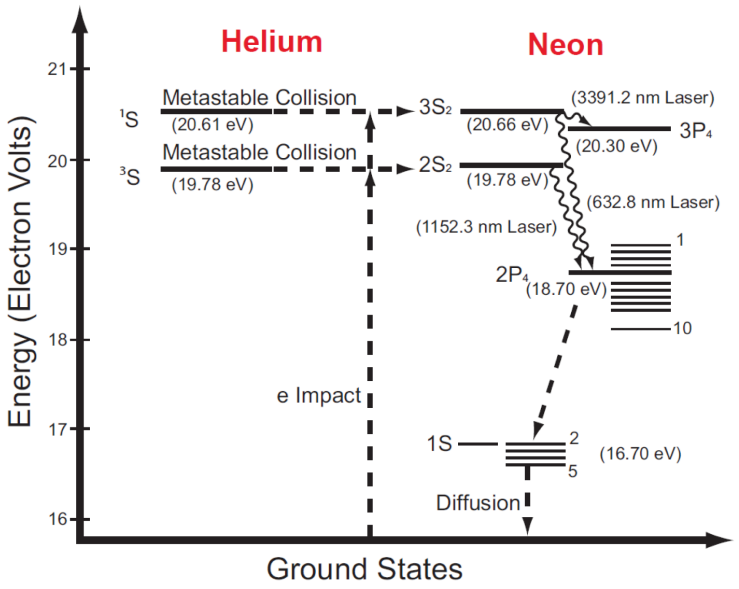


Figure 2.2: He-Ne laser partial energy diagram, presenting the main interations, especially, the lasing transition of $3S_2 \rightarrow 2P_4$, originating the 632.8 nm radiation characteristic of these devices. Image adapted from [26].

The emission of a photon due to an electronic transition between two levels can take place in two ways: spontaneous and stimulated emission. Stimulated emission accounts for the cases in which a carrier that is initially populating a higher level, upon meeting a photon with energy of, approximately, $\Delta E$, will emit a similar photon to the exciting one, while decaying to a lower energy level. The other scenario involving photon emission is the spontaneous emission, where the carrier populating a higher energy level has a chance of spontaneously decay to a lower level which, according to the conservation of energy, requires the emission of a photon with the same energy as the difference between the levels. Many approaches to these mechanisms of generating photons were studied and introduced in the past and recent centuries [28]. Due to the near-constant energy level values in atoms, these subject attracted attention because it would mean achieving highly coherent emission of light, i.e., photons with similar statistics that can be correlated both spatially and temporally [29].

The next main feature required to achieve lasing is the pumping system which has a straightforward but rather important function, necessary to grant light amplification.

As previously stated, the lower energy carriers need to be excited to a higher energy level to then decay and emit the desirable photon. The permanent excitation of these carriers, provided by the pumping system, is also named "population inversion" [28], and is indispensable for the lasing condition.

The final main component of a laser consists in its cavity characterized by having two mirrors on its extremities. In such configuration, when an active medium is present in between the two mirrors, the Fabry-Perot resonator is formed, which requires an optical feedback [27]. When the pumping system elevates the carriers energy, after a relatively small amount of time, they will decay and emit an optical wave that spreads throughout the cavity. Upon reaching a mirror, part of this wave is reflected and a minor percentage is transmitted. The reflected wave then propagates along the entire cavity, promoting stimulated emission. This mechanism defines the resonator and functions as a positive feedback, granting optical amplification. To achieve an optical output, one of these mirrors is set to reflect less than the other one which, consequently, is going to let the light escape through that extremity.

As described earlier, the stimulated emission of light is the responsible mechanism for achieving coherent emission [30]. This phenomena occurs due to the inherent correlation between the carriers that are populating the same energy level. Due to the pumping system of the laser, the carriers populating a higher energy level will decay to a lower one, emitting light to compensate for their loss in energy. As previously stated, the photons emitted by this decay can be triggered via a photon that is already in the cavity. The stimulated photons will acquire the same proprieties as the stimulating one, producing photons with identical waveforms, frequencies, phases and wavelengths, i.e., they are correlated upon stimulation. However, this correlation will not be infinite, neither temporally or spatially, and, as time and travelled distance increase, the correlation between photons decreases and so does the coherence. Temporal coherence is a measurement of the delay time needed to achieve non-correlation between the light emitted at time $t = 0$ and itself measured at another instance [29]. Similarly, spatial coherence is the distance measured during that timeframe, i.e., the distance necessary to achieve non-correlation between the light emitted at the source and the light at another point in space. For a laser light source, where the emission spectrum follows a gaussian profile, the coherence length, $L_c$, and the coherence time, $t_c$, are given by [30]:

$$L_c = t_c c = \sqrt{\frac{2\ \ln(2)}{\pi n_r}} \frac{\lambda^2}{\Delta\lambda}, \tag{2.1}$$

where $c$ is the speed of light, $n_r$ the refractive index of the medium, $\lambda$ the central wavelength of the emission and $\Delta\lambda$ the full width at half maximum relative to the emission peak centered at $\lambda$.

With the rise of highly coherent optical sources, i.e. with a very long $L_c$, the quality of speckle images began to increase and, the more coherent the light source, the more evident the pattern is [30]. Furthermore, in a multimode He-Ne laser, the typical coherence length is about 20 cm [26]. However, in single mode He-NE lasers, the typical

coherence length can exceed 100 m [28]. A laser diode usually has a shorter coherence length of less than a millimeter, while a standard light emitting diode, has very short coherence length, in the order of microns [30]. While evaluating the sharpness and contrast of speckle images, Deng et al. [30] demonstrates that an optical source with a higher coherence length produces higher quality speckle patterns when compared to a lower one, as it can be seen in Table 2.1.

Table 2.1: Quality of the speckle patterns summary based on different optical sources with distinct coherence values according to Deng et al. [30].

| | DPSS Laser[1] | LD[2] | LED[3] | sLED[4] | $\mu$-LED[5] |
|---|---|---|---|---|---|
| Spatial Coherence ($\mu$m) | 112.56 | 91.51 | 22.07 | 12.31 | 5.12 |
| Normalized Spatial Coherence | 1 | 0.92 | 0.76 | 0.73 | 0.56 |
| Normalized Speckle Contrast | 1 | 0.76 | 0.25 | 0.11 | 0.055 |
| Normalized Image Sharpness | 1 | 0.87 | 0.55 | 0.22 | 0.040 |

Diode-Pumped Solid State Laser[1] Laser Diode[2] Light Emitting Diode[3]
Super Luminescent Light Emitting Diode[4] Micro Light Emitting Diode[5]

### 2.1.2 Image Sensor

As previously discussed, optical PUFs devices, contrarily to electronic ones, enforces the need of having an imaging system to collect the response from the PUF when faced with a challenge. In the scope of this work, the imaging system chosen has to correspond to a high resolution device, while being cost-effective for widespread applications. Imaging devices that meet these requirements can be divided in two major categories: CCD and Complementary Metal–oxide–semiconductor (CMOS).

Imaging devices based on semiconductor technology have been dominating the market due to their mobile proprieties, low resolution options, low cost associated with massive distribution, easy-access and relatively accurate imaging systems [31, 32]. While, for several decades, CCD were widespread as the dominant technology, for the past 10 years, CMOS technology evolved and it is now established as the better solution for mobile imaging devices [33]. This market switch was due to advantages of CMOS compared to CCD such as: in-pixel amplification, column-parallel architecture [33], as well as ability to integrate sensing with analog and digital processing down to the pixel level [31].

In Figure 2.3, the differences between CCD and CMOS technologies are highlighted, regarding the different configurations and electronic amplification processes.

Both types of devices take advantage of the photoelectric effect in silicon to generate an electrical signal based on the photons arriving to the pixel surface in the arrays displayed in Figure 2.3 [33]. Although the principles applied to each technology are similar, there are key differences that produce much distinct results. In CCDs, the

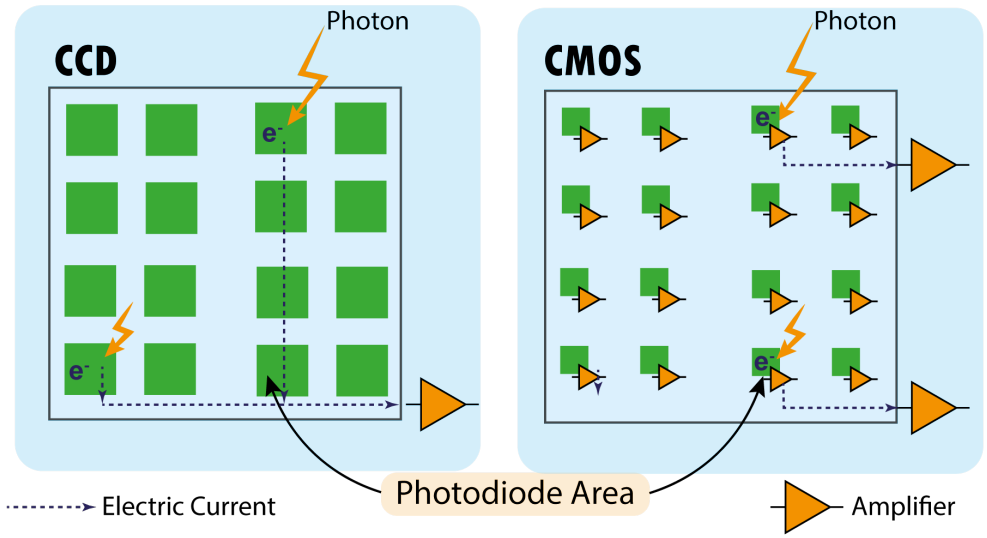


Figure 2.3: Illustration of the processes involved in imaging devices, comparing the CCD and CMOS technologies and their main differences. Note that the incident photon, upon reaching the pixel surface (green) generates an electron ($e^-$) that follows the circuits path, being amplified before the reading in both cases.

photons arriving to the pixels are being converted into a charge that is horizontally or vertically shifted to the extremity of the array. Once it reaches the follower amplifier, the signal is serially read according to the positions in the array. In CMOS, the charge voltage signals are read internally within the pixel, that is also capable of amplifying the signal. The signal is then selected using row/column encoders and transmitted similarly to random access memory circuits. As described so far, both in CCD and CMOS technologies, the pixel is only capable of performing an intensity readout due to its photon-to-charge conversion of all incident radiation. The color interpretation by the system is made by using bandpass filters, which select the colors red, blue and green (in a RGB device) or cyan, magenta, black and white (in a CMKY device) [31]. The filters are placed in front of the designated color pixel in order to block all the other radiation wavelengths that would interact with that pixel, which grants low interference between different color pixels [32].

Naturally, the processes involved in CCD and CMOS imaging are different and both have advantages and disadvantages associated. In CCD, their low-complexity schemes provide image sensors with a smaller pixel area with passive charge transfer, which means that the device will not suffer from fixed-pattern noise and will not induce temporal noise [31]. However, the complexity employed in CMOS grants benefits, namely, a higher signal-to-noise ratio due to its pixel built-in amplifiers. Moreover, the ability of CMOS to perform the signals reading by random access of the pixels, provides a higher processing rate. These advantages of higher readout rate and better SNR, which contributes to a better quality image, motivated many to use CMOS rather than CCD [33].

## 2.2 Physically Unclonable Functions

PUF can be interpreted as a physical entity whose behaviour is a function of its structure and of the intrinsic variation of its manufacturing process [16]. Since the intrinsic variations and manufacturing processes are uncontrollable to some extent, these PUF devices, also known as PUF tokens, assume the propriety of being a physical object with a unique and unpredictable nature [34]. Due to these proprieties, when a PUF device is faced with a challenge, it provides an unforeseeable response which leads to the interpretation of a PUF as a physical one-way function [20]. It is designated CRPs to the pair values $(c_i, r_i)$ that corresponds to the $i$-th challenge, $c$, and response, $r$. The CRPs obtained for each different PUF must differ so it can be considered a unique and unrepeatable device, as it is shown in Figure 2.4.

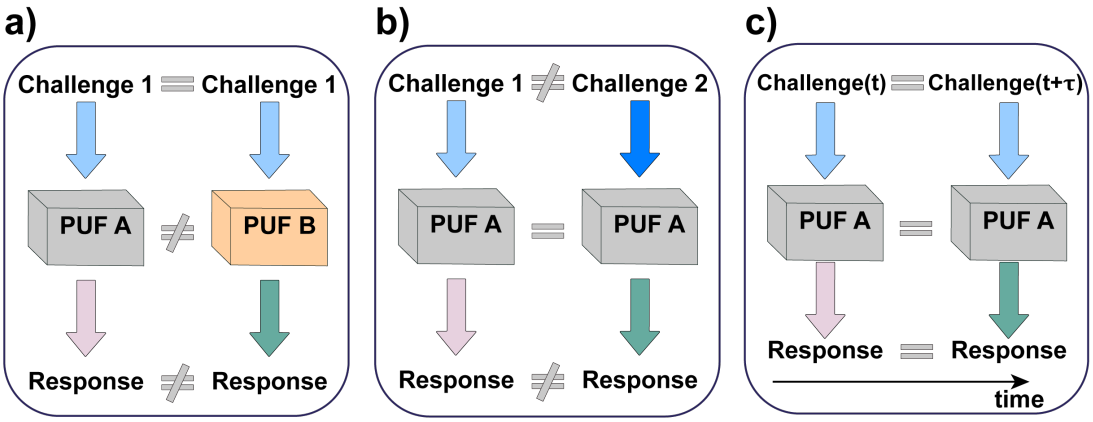


Figure 2.4: Representation of the CRPs expected when different or equal challenges are applied to two different or equal PUF devices. Three different scenarios are represented, featuring common PUF characteristics such as: a) Unclonability: same challenges but different PUFs provide different responses, b) Unpredictability: different challenges to the same PUF provide different response and d) Robustness: time-invariant operation. Image adapted from [14].

To summarize, the fundamental requirements to be considered while classifying any object as a PUF are [35]:

- Uniqueness: due to the objects microstructural variation, dependent of unpredictable manufacturing conditions, a unique output is expected for each unique device.
- Unclonablility: attempting to duplicate a PUF should result in an identical object. However, this object is expected to produce a different CRP when compared to the original. Therefore, the inevitable structural randomness avoids PUF cloning attacks.
- Unpredictability: Based on previous records of CRPs, given $(c_i, r_i)$, one cannot predict the outcome of $(c_k, r_k)$ when $i \neq k$, without querying $c_k$ and recording $r_k$.

- One-way: given $r_i$, it is infeasible to recover the paired challenge $c_i$ that originated $r_i$. However, by applying $c_i$ to the PUF device, one can expect the response to be $r_i$.

- Tamper evident: attempting to alter the PUF structure would result in a variation of the PUF features, returning a different CRP, when compared to the original CRP, indicating that the sample was tampered.

As stated in Chapter 1.3, PUFs can have a variety of applications, from product tagging being implemented as a counterfeiting safety measure, to being integrated in cryptographic systems, performing both random number generation and authentication protocols. The viability of these devices must also fulfill key requirements. In 1883, Kerckhoffs [36] enunciated the fundamental principles applicable to cryptographic systems that can be listed as:

- the system should be practically indecipherable, if not mathematically.

- the existence or functioning of the system must not be a secret.

- it must be easy to communicate, retain and change (when required) the key involved in the operation.

- the system ought to be compatible with telegraphic communication systems.

- the system must be portable.

- the system must be user-friendly - where the operation/interaction with the system does not entail significant skill acquisition or effort.

Attending that PUFs do have the characteristics described above that makes them a strong solution for a secure device to be integrated in a cryptographic system [37], they also present advantages that distinguish them from other common solutions, such as:

- presented as a high potential alternative to be implemented in cryptographic key storage technologies due to their resistance to tampering and programmed assaults, while having a lower cost when compared to other technologies.

- since the keys are generated due to the intrinsic random process variations of the tokens, the threat of information leakage or negligence from the system owner/manufacturer is eliminated and the key cannot be compromised by an untrusted third party, increasing the security of these devices.

- mass-cloning is also impractical, considering the nature of the devices, thus making PUFs a reliable help against targeted attacks.

- PUFs do not require any special fabrication for key storage purposes, while also being scalable security entities regarding their size and shape.

In the analysis made in Section 1.3, different types of PUF devices were reviewed that fulfilled the requirements described above. In that review, the PUF types were distinguished, namely, in electronic PUFs and optical PUFs. While electronic PUFs take advantage of the unique physical variations that occur during semiconductor manufacturing [17], optical PUFs generally evaluate the speckle pattern produced via the interaction between a coherent light source and a physical device. Although both configurations follow some of the same principles, such as, being a unique, unclonable and unpredictable device, their principle of operation differ greatly which than is reflected in important differences.

As previously stated, in this work, optical PUFs and their implementation are focused on regarding their performance and security over other typical methods of cryptographic key distribution. They were first introduced in [20], which pointed to some advantages that the optical integration of these tokens can have when compared to electronic PUFs [17]. Firstly, the cost of an optical token to be used as an optical PUF can be drastically low since the token could only be an inexpensive plastic structure, with no particular feature. Contrarily to electronic PUFs, in this case, there are no requirements for the usage of microelectronics or silicon circuits to process such token, which will greatly impact the cost of an optical token. In addition to that, a simple plastic token can produce a high complexity output since each PUF consists in numerous surface imperfections which can lead to a very complex optical interference process inside the token. Moreover, as [17] indicated, these optical PUFs, when compared to electronic ones, offer a higher security against modeling attacks. Modeling attacks to a PUF device is when an attacker, who possesses a large database of the characteristic CRPs, is able to develop a program capable of estimating and predicting the PUFs response under different circumstances. In terms of cloning attacks, the optical PUFs are also reported to have a higher security and are suited as "Certifiable PUFs", i.e., within certain limits, it has been proven that these devices cannot be modified or exchanged by malicious parties [17]. Inherently, a trade-off is established when using optical PUFs since they require an optical precision imaging system to perform the readout of information. This mechanism must establish exactly the same relative positioning of the light scattering token, the laser beam, and the CMOS camera upon every single readout, making its implementation expensive and potentially error prone, while also being a demanding task when trying to miniaturize the system or assembling a portable one.

### 2.2.1 Hashing Process

While optical PUFs present a solution for image-based authentication and cryptographic key generation, the response generated by these devices needs to be clearly represented to be mathematically processed [38]. To achieve this, one can reduce the

response produced by the PUF into a bit string for further evaluation using a hash function. Since the processing being developed in this work is related to optical PUFs, where the response to the PUF challenge is an image, the hashing is adapted to a perceptual hash function [39]. The image perceptual hashing is the process where, given a certain output image, a bit string is calculated based on the human perception of that image. While perceptual hashing does not consider all the image data, the advantage of such interpretation is that the principal characteristics of the image are analysed. For example, images that suffer transformations such as added noise, compression, different brightness and rotations all produce the same hash, i.e., slightly different responses are identified as the same PUF object [40].

Hash functions can have multiple purposes and implementations such as one-way mathematical functions to block reverse engineering attacks, as encryption functions with a secret key shared between provider and user, to ease signal and image processing in digital systems, and variations or combinations of these intents [41]. In the scope of this work, the perceptual image hashing will be used both to reduce and classify image data, as well as to compare different PUF responses, establishing the authentication protocols.

In this work, the hash function used is the type-II DCT and has the definition [42]:

$$F(k) = \sum_{n=0}^{N-1} c(k,n) \cdot f(n), \tag{2.2}$$

where $F(k)$ represents the DCT sum, $k$ the number of bits used in the DCT calculation, $c(k,n)$ the DCT coefficients, $n$ is the sample index of an input signal with size $N$ and $f(n)$ the input signal. According to the definition given by Shin et al. [42], the DCT coefficients, $c(k,n)$ are established such as:

$$c(k,n) = \sqrt{\frac{2}{N}} \cos\left(\frac{\pi k(2n+1)}{2N}\right). \tag{2.3}$$

Using the $c(k,n)$ notation for the DCT coefficients calculated for the given input $f(n)$ size, one can apply Equation (2.2) to a given image, $I$, constructing the DCT matrix of the image, $I_{\mathrm{DCT}}$:

$$I_{\mathrm{DCT}}(I) = c \cdot I \cdot c' \tag{2.4}$$

where $c'$ represents the transpose of the $c$ matrix. The DCT matrix generated via this method as some inherent proprieties due to the formulation described in Equation (2.2). The upper left terms of the matrix correspond to the low frequency terms in the image, while the lower right coefficients are associated with high frequency terms. In Figure 2.5, the image DCT matrix is described, highlighting the placing of the different frenquency coefficients.

While the entire representation of the matrix yields the best image reconstruction to the smallest detail, most of the applications (for example television broadcasting,

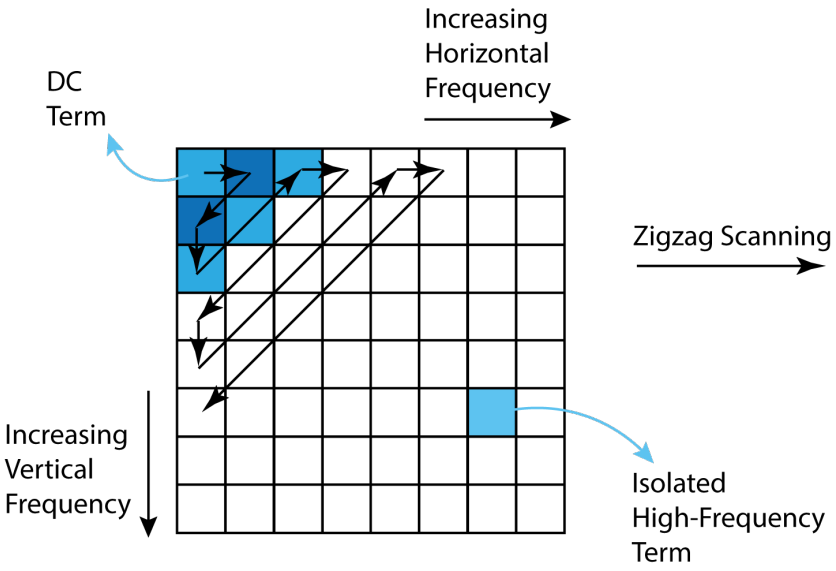


Figure 2.5: Representation of the type-II DCT matrix, focusing on the frequency increase with the number of rows and columns and also highlighting the zigzag scanning method which retrieves, by order, the lowest frequency terms of the matrix.

software image compression and cryptographic systems) take a smaller portion of this matrix for their interpretation [43]. This work was focused on the upper left coefficients of the image matrix since those are the best coefficients to generally represent the picture, while neglecting the higher frequency terms that are associated to minor changes that do not affect the human perception of the image. To achieve this selection, the method used was Zig-zag scanning, with a MATLAB® routine implemented in [44] and also represented schematically in Figure 2.5. The number of coefficients attained by this method will depend on the systems proprieties and different approaches will be considered to determine the optimal number of coefficients [45].

Taking into consideration the formulation presented in Equation (2.2), the number of coefficients extracted from the image DCT matrix is the number of bits considered for that image when performing the key extraction. Consequently, by having a longer key generated by each output of the PUF device, it will also enforce that higher frequency coefficients are used to identify that key. Therefore, a compromise needs to be established where for each image, a certain number of bits are extracted with significance while associated to the lower frequency coefficients of the DCT matrix.

After the extraction of the lower frequency coefficients of the image DCT matrix, $C_i$ using zig-zag scanning, a decision as to be made for each of those coefficients that will construct the key. Note that, in this formulation, the first DCT coefficient, illustrated as the DC term in Figure 2.5, is not considered due to the redundancy of this term in every image which would weaken the key extracted. Let $m_d$ be the mean value of all

the coefficients $C_{i,i\neq 1}$, then the hash values, $h_i$, for the key are given by [46]:

$$h_i = \begin{cases} 0, & C_i < m_d \\ 1, & C_i \geq m_d \end{cases}. \tag{2.5}$$

As for the quantification of the PUF performance, the most used figure of merit across PUF implementations is the hamming distance. This quantity evaluates the bit strings retrieved, $h_2$, from the response of the PUF and compares them to the bit strings expected by the device, $h_1$. During this work, the normalized hamming distance (HD) was used and it is defined by [47]:

$$\text{HD} = \frac{1}{N} \sum_{n=1}^{N} |h_1(n) - h_2(n)|, \tag{2.6}$$

where $n$ is the bit index up to a maximum of $N$ bits transmitted. In Figure 2.6, an illustration is presented to highlight both the hash extraction technique using the DCT matrix image and the posterior processing of the comparison between hashes, using the hamming distance metric.

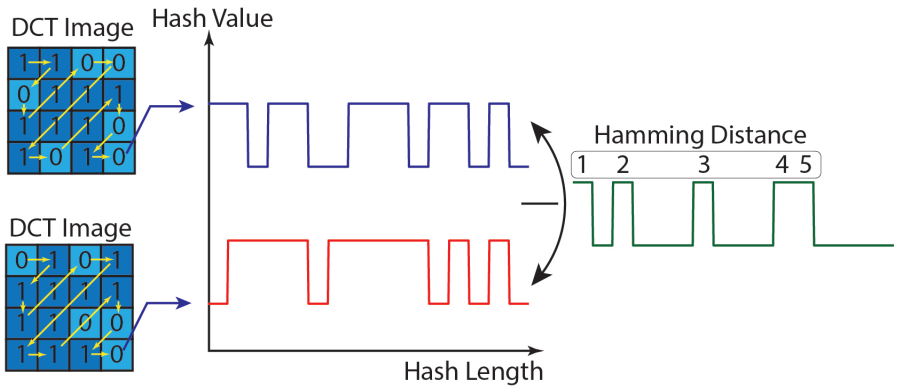


Figure 2.6: Illustration of the hash function extraction using the DCT matrix to then evaluate the hamming distance. Note that the normalized hamming distance, divides the number of different bits by the total hash length.

Throughout this hashing process, the exemplification of the key extraction was targeted to a unique image of the PUF device and that response was compared to the expected one. However, this analysis can be considered to a set of multiple images, for example, applying these methods to the frames of a video. The advantage of retrieving multiple hamming distances of the authentication device is to be statistically confident that the device in question is qualified or not to access the information. In many applications, these hamming distances are represented in a histogram and are well described by a Gaussian probability density function with a mean ($\mu$) and variance ($\sigma^2$). The lower the mean value of the Gaussian curve, the more likely the device is to be authenticated and narrower the curve, the more likely the decision of authentication

is to be correct. The main characteristics of the hashing process used in this work are schematized in Figure 2.7.

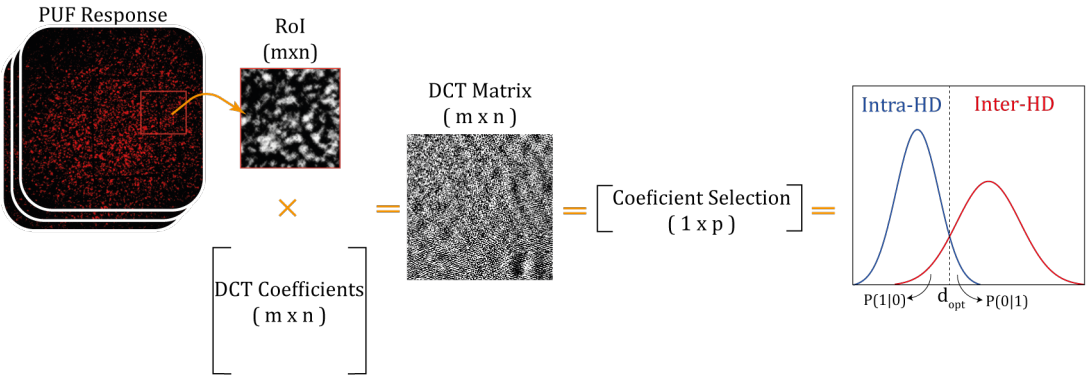


Figure 2.7: Diagram exemplifying the hashing process involved in processing multiple PUF responses. In this case, a variety of PUF responses are cropped taking into consideration a pre-designated Region of Interest (RoI) and transformed into a red-scale image. Combining this images with the DCT formulation, the DCT matrix is calculated. The coefficients of the DCT matrix are retrieved using the zigzag scanning method and are afterwards compared with the original image which returns the hamming distance to later be compared using the decision threshold applied.

To apply a quantitative metric to the decision threshold and authentication process, a "maximum-likelihood" decision criteria is used to determine the decision threshold, $d_{\text{opt}}$, and the error probability, PoE, associated with the identification of PUF devices, described in [48]. In this case, the authentication key stored in the database that originated from device "A", is compared to the key generated from device "B" that is to be authenticated. Assuming that the process in Figure 2.7 is followed, the final results will yield 2 Gaussian distributions based on the hamming distances calculated, one when the devices "A" and "B" are identical (intra-HD) and another for distinct devices (inter-HD). These distributions, for both device "A" and "B", will be characterized by having a mean value, $\mu_a$ and $\mu_b$, and a variance, $\sigma_a^2$ and $\sigma_b^2$, that can be used to calculate the optimal decision threshold:

$$d_{\text{opt}} = \frac{-(\mu_a\sigma_b^2 - \mu_b\sigma_a^2) \pm \sqrt{(\mu_a\sigma_b^2 - \mu_b\sigma_a^2)^2 - (\sigma_a^2 - \sigma_b^2)(\mu_b^2\sigma_a^2 - \mu_a^2\sigma_b^2 - 2\sigma_a^2\sigma_b^2\ln(\frac{p_b\sigma_a}{p_a\sigma_b}))}}{(\sigma_a^2 - \sigma_b^2)}, \tag{2.7}$$

where $p_a$ and $p_b$ are the bit probabilities associated with the intra-HD and inter-HD distributions. Note that, in this case, it is assumed that $p_a = p_b = 0.5$, which represents a 50% probability of considering an intra-HD or inter-HD entry.

After a threshold level as been deployed and the authentication decision been made, one can infer at PoE that arises from such decision. This probability can be calculated

as:

$$\mathrm{PoE}(d(h_a, h_b)) = \frac{p_a}{\sqrt{2\pi\sigma_a^2}} \int_{-\infty}^{d_{\mathrm{opt}}} \exp(-\frac{(x-\mu_a)^2}{2\sigma_a^2})\, dx + \frac{p_b}{\sqrt{2\pi\sigma_b^2}} \int_{-\infty}^{d_{\mathrm{opt}}} \exp(-\frac{(x-\mu_b)^2}{2\sigma_b^2})\, dx\,. \tag{2.8}$$

The equation described in (2.8) analyses the integrated normalized gaussian curves with respect to the hamming distance. Furthermore, the PoE can be understood as the sum of the probabilities of misinterpreting a bit "1" as a bit "0", P(0|1), and the probability of misinterpreting a bit "0" as a bit "1", P(1|0). It is denoted False Positive Rate (FPR) to the probability P(1|0), while P(0|1) is called False Negative Rate (FNR), which are directly influenced by the performance of the system, as highlighted in Figure 2.7, considering that the threshold level chosen is $d_{opt}$, described in Equation (2.7).

To test the ability of perfectly distinguish two PUF devices, one has to quantify their total "likeliness". To accomplish so, consider two devices, $A_i$ and $B_m$, that, when faced with a challenge, produce the responses $r_i$ and $r_m$, respectively. Note that, in this formulation, the device $A_i$ is considered to have a response $r_i$ that is incorporated in a database since it will be the predicted authentication response. Ideally, if device $A_i$ is different from device $B_m$, their responses, while facing the same challenge, should differ completely, yielding a close to 0.5 normalized hamming distance. Across multiple responses of the devices to numerous challenges, the devices demonstrates *uniqueness* if the $\mathrm{HD}(A_1, B_2)$ is close to 0.5 [49]. Contrarily, if $\mathrm{HD}(A_1, B_2)$ presents a value close to 0, it is concluded that the devices are not unique, i.e., they are the same device. To calculate the *uniqueness* across a total of $M$ devices and $N$ total number of acquisitions, one should determine:

$$EC = \frac{1}{M(M-1)N} \sum_{i=1}^{M} \sum_{m=1, m\neq i}^{M} \sum_{j=1}^{N} \frac{\mathrm{HD}(r_i, j, r_m)}{k} \times 100\%, \tag{2.9}$$

where $k$ is the number of bits extracted in the type-II DCT matrix construction.

All of the descriptive methods mentioned thus far, will be explored and applied to characterize the PUF tokens implemented under the scope of this work.

# CHAPTER 3

## PUF Experimental Implementation

In this chapter, it will be detailed the experimental implementation steps required to produce and acquire images of speckle as well as a description of the PUF tokens used and optical components, highlighting their most important features in the scope of this work. Lastly, both speckle analysis algorithms will be disclosed.

## 3.1 PUF Tokens

As previously stated in Section 2.2, a PUF arises from the intrinsic proprieties of a physical object and, in this case, the interaction of this object with a coherent light source. This experimental implementation will be focused on three different objects and their respective speckle responses, mainly to determine their viability, performance and quality when used as a PUF device. To understand how the microstructure of these tokens can induce a speckle pattern, Figure 3.1 was elaborated combining the microscopic images of each token, attending on their individual microscopic features that identifies them as PUF devices.

One of the tokens studied was the tracing paper and two different samples (A and B) were considered, hereafter called p-PUF$_{\mathrm{A,B}}$. The tracing paper samples, with dimensions 6×6 cm, are nonwoven polyester paper fabrics which is made from 100% recycled polyester that is characterized by being water resistant, capable of withstanding high mechanical strain and with a density of 250 g/cm$^2$. The choice of tracing paper as a PUF was made because it is a translucent object, which means that part of the laser light will be easily transmitted, resulting in a viable and noticeable speckle pattern while using a low-cost solution for testing the experimental setup. However, a careful implementation of this device was conducted to prevent changes in the speckle pattern, since the paper is very susceptible to external stimulus such as wind and gravity, that would continuously change the paper position, inducing different speckles.

Another PUF token implemented during this work was a 1.5 cm plastic optical fiber segment (Ref. HFBR-RXXYYYZ by Broadcom), where two samples (A and B) were considered, named f-PUF$_{\mathrm{A,B}}$. While using a 660 nm light source, this plastic optical fiber, has an attenuation of 0.22 dB/m and it is used in a variety of applications from telecommunications to industrial automation. It has a reasonable thermal stability, able to be stored between -55$^{\mathrm{o}}$C and 85$^{\mathrm{o}}$C without any degradation. The core of the step-index fiber, $n_r = 1.492$, has a diameter of 1 mm and the jacking has a diameter of 2.20 mm, made with polyethylene ($n_r = 1.417$). This fiber is also characterized

by having a numerical aperture of 0.5 and a propagation delay of 5 ns/m. This device was chosen due to the ease to observe a speckle pattern, allied to the low-cost implementation and access of these fibers. Another significant advantage is that these fibers have a well-defined numerical aperture which benefits greatly the quality of the speckle pattern. As it can be seen in Figure 3.2, the f-PUFs were placed in a custom made metallic structure that provides mechanical stability and facilitates the reproducibility and consistency of the results.

Lastly, most complex token used was a monolith shaped sample made with d-U(600) di-ureasil containing $Eu(tta)_3 \cdot 2H_2O$, hereafter named m-PUF, fully described in [50]. While this device is not as accessible as the others, it poses several advantages such as: the possibility of assembling the samples in a variety of shapes to fit different applications, higher unclonability due to the processes involved in their fabrication and the high transparency profile of the samples which can be useful in optical applications.

The compound synthesis was performed by Dr. Lianshe Fu, at CICECO - Aveiro Institute of Materials, and consisted on the incorporation of the $Eu^{3+}$-doped di-ureasil hybrid, which is a process that involves two steps. The first one related to the formation of the urea cross-linked organic-inorganic hybrid precursor, diureapropyltriethoxysilane. In the second step, $Eu(tta)_3 \cdot 2H_2O$, with the synthesis described in [51], was incorporated as an ethanolic solution together with water and hydrochloric acid, HCl. Note that in the case of this device, instead of manufacturing a similar sample to be designated sample "B", different surfaces of the monolith were used to produce the speckles "A" and "B", providing that a rotation of the monolith with respect to the laser beam would generate a completely different speckle pattern.

The m-PUF token presents numerous advantages to be considered for cryptographic and remote key storage purposes. In a environmental and sustainable context, the organic-inorganic hybrid was processed at room temperature which indicates that the sample has high stability in harsh media and that is applicable for large-scale production due to its energy efficient synthesis [50, 52]. Di-ureasils are also characterized by being processed using environment-friendly green solvents with tuneable viscosity, which makes them ideal low-cost and sustainable materials [51]. Moreover, this token can be developed with the desired shape and thickness, which combines the flexibility of the organic counterpart with the mechanical stability of the inorganic one [51]. Among the different organic-inorganic hybrids, the emphasis is given to di-ureasils, whose siliceous-based skeleton provides compatibility with current microelectronics and confers enhanced thermal stability with the onset of the decomposition temperature at 339$^{o}$C compared with pure polymer-based host (such as the p-PUF) [51].

The microscopic images, presented in Figure 3.1, in bright field mode were recorded using an Olympus BX51 microscope equipped with a digital CCD camera (Retiga 4000R, QImaging) used to capture the microphotographs of the samples in reflection or transmission mode under white light illumination of a DC regulated illuminator (DC-950, Fiber-Lite).

In Figure 3.2, all the tokens used are displayed, highlighting the individual place

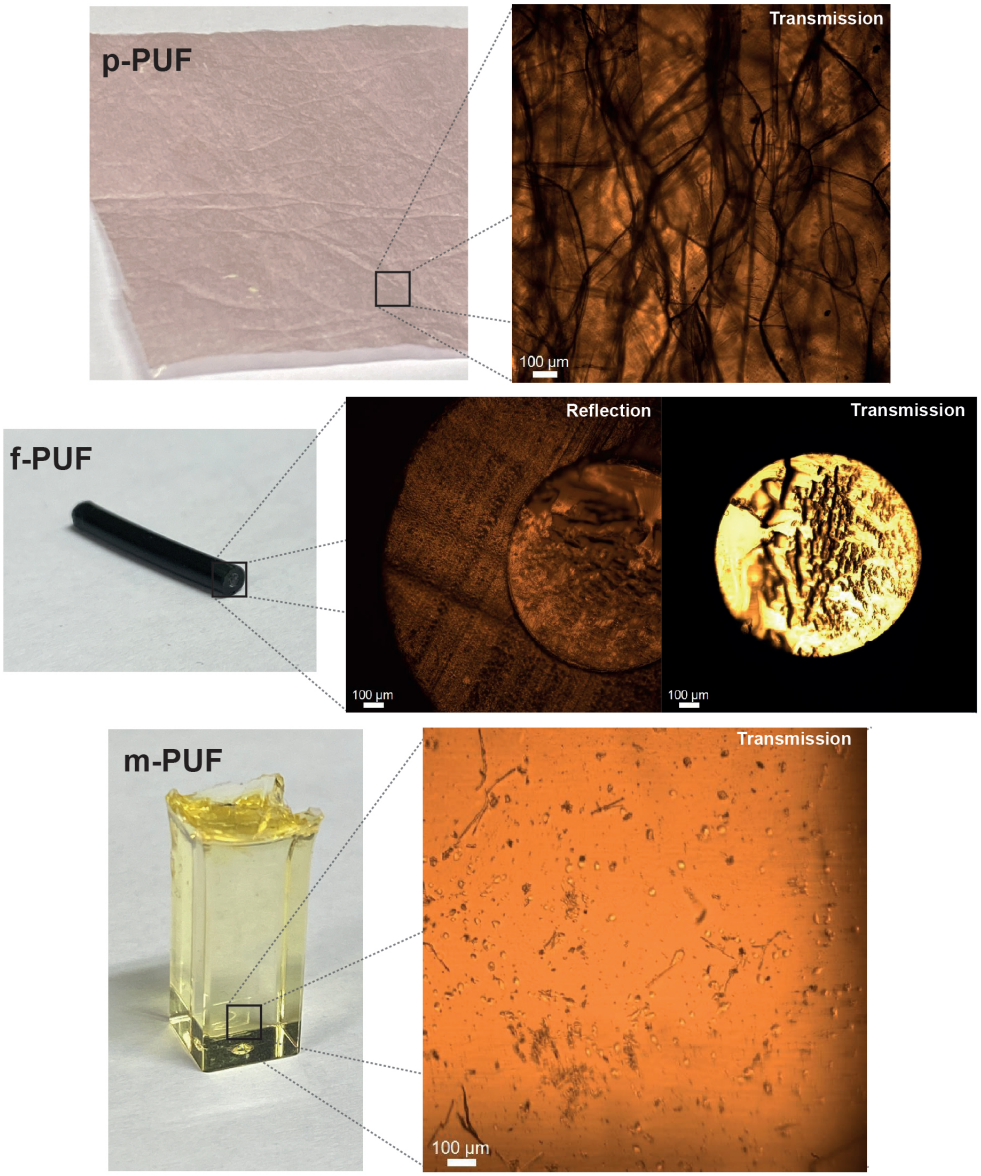


Figure 3.1: Photographs of the p-PUF, f-PUF and m-PUF tokens utilized during this work. The highlights were captured with microscopic images of the tokens using an Olympus BX51 microscope equipped with a digital CCD camera (Retiga 4000R, QImaging) used in reflection or transmission mode under white light illumination. The microstructures of these tokens are directely responsible for speckle pattern formation under the illumination of coherent radiation.

holders created to suit their proprieties. With the p-PUF, an effort was made to assure that all the external light sources were blocked and that the tracing paper was placed in a mechanically stable structure to prevent fluctuations in the speckle pattern that would, inevitably, induce negative changes in the performance results. While using the f-PUF devices, a custom made metallic structure was constructed to fit the segments of the plastic optical fibers and to also provide mechanical stability which facilitates

the reproducibility and consistency of the results, while also blocking external light sources. Lastly, a regular cuvette was wrapped in black tape with a small orifice to, once again, diminish the interactions of external light sources that would arise while using the m-PUF device. In this particular case, the two devices integrating in m-PUF are two different surfaces of the same monolith, as it can be seen in Figure 3.2.

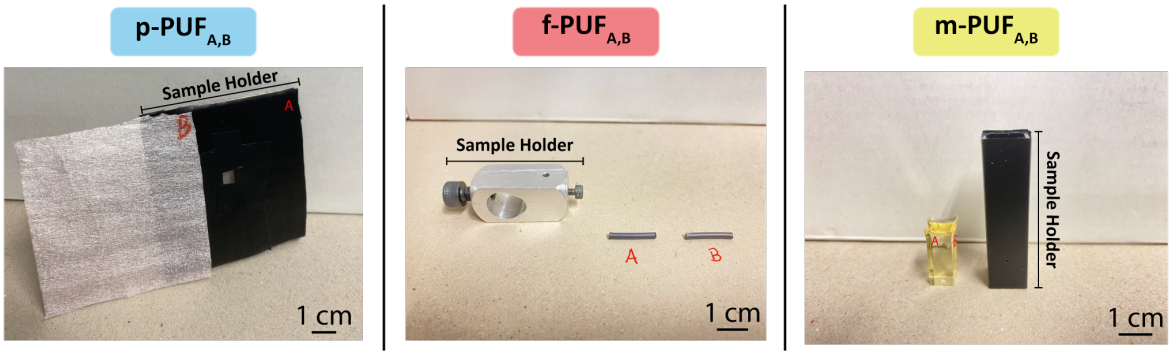


Figure 3.2: Images of the three types of PUF devices studied in the scope of this work. The p-PUF device is placed under a mask which is a compact structure covered with black tape to prevent interactions with different light sources other than the laser. In f-PUF, the samples are set in a small custom made orifice to assure a stable placement of the fibers. Finally, the m-PUF device is placed inside a cuvette, also covered in black tape, with a small orifice with the size of the laser beam in order to guarantee only a speckle pattern based on a specific location of the sample.

The implementation of the PUF devices and posterior characterization requires a concise and uniform method of sample identification that will be used throughout this work and, thus, Table 3.1 was elaborated to summarize all the different tokens used, as well as to disclose their compositions and designations used for each individual speckle response.

Table 3.1: Summary of the PUF tokens considered in the scope of this work, with their respective compositions, sample denotation and the designations applied to each response.

| PUF token | Composition | Samples | Response | Designation |
|---|---|---|---|---|
| Tracing Paper | Nonwoven Polyester Paper Fabric | A | 1 | p-$PUF_{A,1}$ |
| | | | ... | ... |
| | | | 40 | p-$PUF_{A,40}$ |
| | | B | 1 | p-$PUF_{B,1}$ |
| | | | ... | ... |
| | | | 40 | p-$PUF_{B,40}$ |
| Plastic Optical Fiber | Sigle Step-index core fiber with Polyethylene jacking | A | 1 | f-$PUF_{A,1}$ |
| | | | ... | ... |
| | | | 40 | f-$PUF_{A,40}$ |
| | | B | 1 | f-$PUF_{B,1}$ |
| | | | ... | ... |
| | | | 40 | f-$PUF_{B,40}$ |
| Organic Inorganic Hybrid | Di-ureasil hybrid containing $Eu(tta)_3 \cdot 2H_2O$ | A | 1 | m-$PUF_{A,1}$ |
| | | | ... | ... |
| | | | 40 | m-$PUF_{A,40}$ |
| | | B | 1 | m-$PUF_{B,1}$ |
| | | | ... | ... |
| | | | 40 | m-$PUF_{B,40}$ |

## 3.2 Experimental System

The experimental system used to produce and record the speckle-based images of the PUF devices studied is described in Figure 3.3.

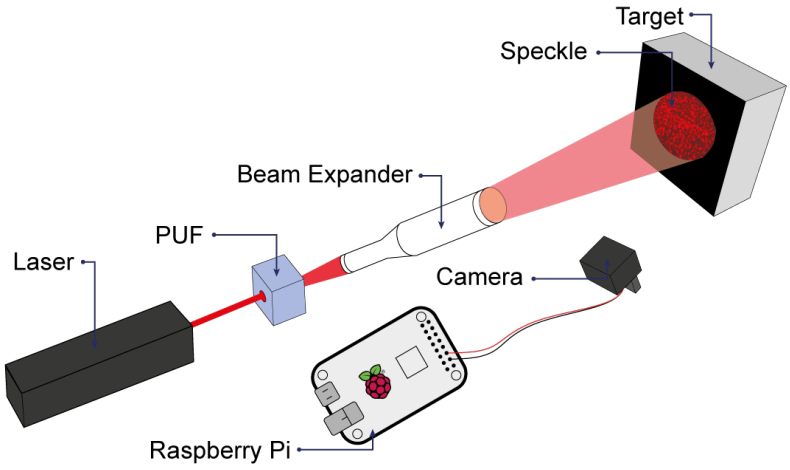


Figure 3.3: Illustration of the experimental system used to produce and acquire speckle images based on PUF devices.

As in any other optical system, it is very important to assure that all the components are carefully aligned to their purpose. In this case, the laser, PUF device and beam expander must all be perfectly aligned so that the speckle image is reproductible the next time a user tries to measure the response of the PUF, when faced with this laser challenge. An incorrect alignment of this components, for example by a certain angle, will induce changes to the speckle image, introducing another degree of freedom to the system which can pose unnecessary complexity. It is also important to point out that the "PUF" component described in Figure 3.3 is a generic representation of any PUF device that is desired to be implemented, granted it can produce a noticeable speckle pattern. The beam expander, also represented in Figure 3.3, is the GBE20-A - 20X Achromatic Galilean Beam Expander (by Thorlabs) and it is used to expand or reduce the diameter of an incident collimated beam. Although the integration of this component constitutes an increase in complexity of the system, it also plays an important role in increasing the quality and sharpness of the speckle images. In fact, for devices (such as the m-PUF) that produce smaller grain-sized speckles, the beam expander proves to be efficient in enhancing the size of these speckle patterns, contributing to a better implementation of such devices. As for the "Target", a plain white regular surface (printing paper) attached to a metal structure was chosen to display the image since it improves the speckle signal by reflection while minimizing possible external alterations to the speckle pattern. Although it was stressed that the alignment was a key factor in the implementation of optical PUF devices, as for the camera position, a small angle must be considered so that the physical structure of the camera would not block the speckle pattern. However, not only this angle was

reduced to the minimum required to eliminate light blockage, it was maintained fixed during all the experimental data acquisition so that this factor would not interfere in the interpretation of the results. Lastly, the camera was connect to a Raspberry Pi board, as previously discussed, creating a compact and portable system for PUF authentication. Although it is not represented, the Raspberry Pi is equipped with all the peripherals needed to store the images.

To introduce random variability in the image acquisition process, between every recorded speckle pattern, both the laser and the camera were reset. This factor was introduced to guarantee that every user could retrieve, from the same PUF device, a similar, or preferably equal, hash function upon the image characterization, regardless of external factors.

The light source used to produce speckle-based imaging of PUF devices was a coherent He-Ne Laser (ref. HNLS008R by Thorlabs [26]). With respect to the laser safety guidelines, this laser is a class IIIA, considered to be safe when handled carefully [26]. In terms of maximum optical output power, the laser is expected to achieve 2 mW, characterized by having an emission line of 632.8 nm. Other features to consider are the beam diameter which is 0.48 mm, beam divergence of 1.7 mrad and a coherence length of 30 cm. Although this laser has a 20 cm cavity, making it a sizable light source alternative, it produces a stable optical output power, with a well defined beam profile which is ideal to use in applications where the results, in this case an image, are highly sensitive to the lasing performance.

The speckle image acquisition system, which can be seen in Figure 3.4, was developed using the Camera Module V2 connected to a Raspberry Pi, model B with 512 MB RAM, powered with 5V at 1.2A, and working on Raspberry Pi OS. Not only the camera module is fully programmable in the Raspberry Pi OS environment, it is also characterized by having a CMOS 8-megapixel image sensor developed by Sony (ref. IMX219), being capable to capture 3280 x 2464 pixel static images and having an optimized unscrewing lens to change the focal distance from 80 to 280 mm [53].

The advantage of using the Raspberry Pi along with the supported camera is the possibility of having a fully programmable imaging system that is compact, low-cost, user-friendly and fully independent. Combining these advantages with the fact that this micro-controller supports internet connection, it is possible to have a system connected to a database while performing real-time PUF authentication without any user input.

The entire code for image acquisition purposes was developed in Python that can control all the proprieties of the camera module. In addition, these camera proprieties were tested in the system to check their viability and quality in registering the produced speckles. The numeric values of these proprieties are described below and were used for all image acquisition data throughout this entire work:

- ISO: which stands for International Standards Organization, is the sensitivity to light as pertains to either film or a digital sensor. This value was set to 800 as it is the maximum sensitivity obtain using this device.

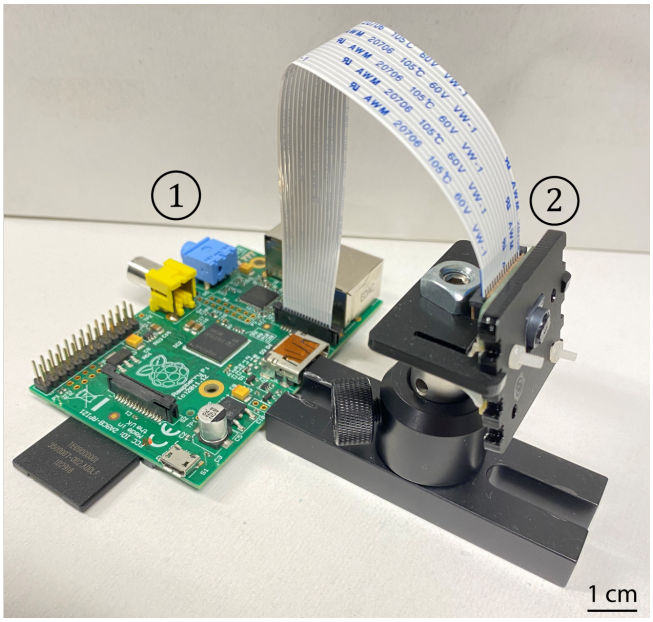


Figure 3.4: Photography of 1) Raspberry Pi 1, model B with 2) Camera Module V2 attached. The camera is incorporated in a custom adjustable mount that is compatible to arrange in a optical table, to provide high-precision positioning.

---

- Brightness: sets the pixel intensity across the image. Ranging from 0 to 100, this value was set to 60 to induce brighter pixels in the pattern.
- Contrast: determines the difference between the colors in the image. A higher contrast image will consist of a small number of color levels, for example, a black and white picture. Ranging from -100 to 100, this value was set to 100 to produce high contrast images since it produces clearer speckle patterns.
- Exposure Compensation: a common feature used to produce darker or lighter images. Ranging from -25 to 25, this value was set to 25 in order to acquire brighter images due to the low light intensity of the system.
- Shutter Speed: is the amount of time that the shutter of the camera spends open recording the light. Naturally, a faster shutter speed implies a lower exposition time. This value was set to the maximum available, 33 milliseconds, to have a brighter and more defined image.
- Saturation: measure of how pure is the color in the image. A high saturation represents a true color while low saturation turns the color gradually to black by adding gray. Ranging from -100 to 100, this value was set to 30 in order to obtain a slightly clearer image of the red color from the laser.
- Sharpness: can be interpreted as the distance needed to change the intensity of a pixel and its the contrary of blur. Ranging from -100 to 100, this value was set to 100 in order to better distinguish high intensity pixels from low intensity ones.

Moreover, it is important to note that some of the programmable aspects of the camera module are only recognized if some proprieties are set to "*off*" to prevent automatic regulation from the camera itself. As a result, "*awb_mode*", which controls the white-balance of the camera and "*exposure_mode*", predefined camera exposure definitions, were previously set off to enable the user to program both the white-balance and exposure of the camera.

As previously stated, before acquiring the speckle images, a test of the parameters of the camera was conducted to ascertain their optimal values. In Figure 3.5, two images, acquired using default and customized parameters, are shown to reflect their importance in the final results.

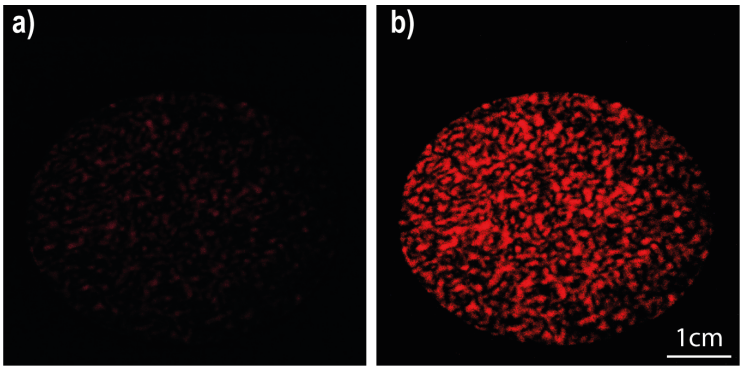


Figure 3.5: Speckle images acquired using the p-PUF token comparing a) the default camera capture parameters and b) the custom optimized parameters used, while maintaining constant the shutter speed (33 ms). In image a), the default camera parameters are: brightness(50), ISO(100), saturation(0), sharpness(0), exposure compensation(0), contrast(0). The custom optimized parameters used in b) are: brightness(60), ISO(800), saturation(30), sharpness(100), exposure compensation(25), contrast(100).

Figure 3.5 illustrates the importance of setting the camera parameters to optimal values depending on the environmental conditions. Throughout the entirety of this work, the camera parameters applied in image 3.5b) will be used and the lighting conditions surrounding the system will be identical (low illumination) to acquire reproducible, comparable and consistent results.

## 3.3 Speckle Pattern Processing

After the speckle images were acquired by the camera and loaded into the Raspberry Pi, the next step was to apply multiple routines in order to extract the hash function and to execute performance and authentication analysis. In line with the objectives proposed, MATLAB® scripts were created and implemented, emulating the user authentication process that queries the database, as schematized in Figure 3.6.

In this algorithm, firstly, it is considered that the PUF device to be authenticated, i.e. requiring a "User Verification", will have a response to the laser challenge that

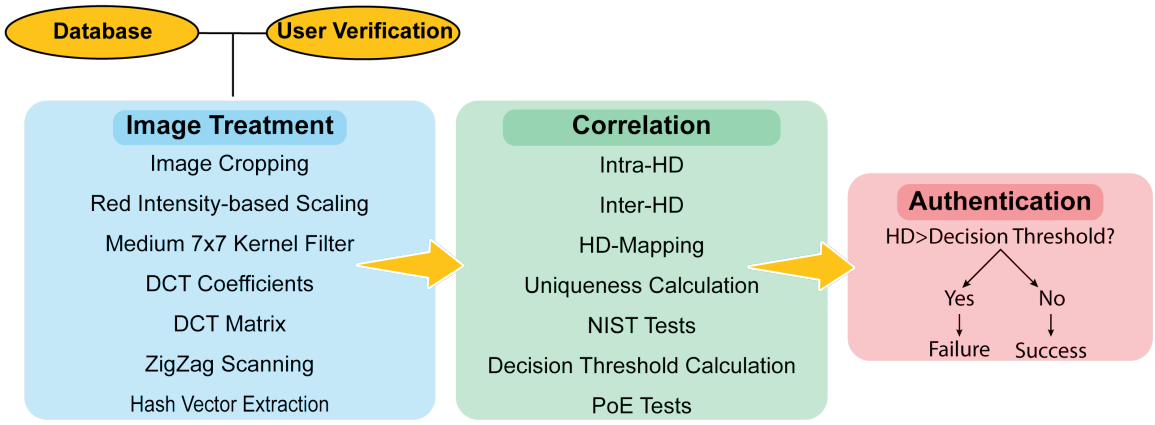


Figure 3.6: Diagram of the different phases implemented in the MATLAB® routines that constitute the PUF analysis algorithm.

will be compared to the response stored in the "Database". The first step to identify and treat the response from the PUF device is to perform a series of image treatment algorithms. The image treatment algorithm begins by cropping the image to a RoI that is the same frame of reference for all the other images. By doing so, it is guaranteed that the hash vector extraction comes from the same pixels of the database image and the newly recorded image. Next, from the RoI selected, it is only considered the red intensity of the pixels which matches the laser emission and reduces the complexity of the image. The application of the medium 7×7 kernel filter is to minimize the difference between the reconstructed frame and the original frame, i.e., reducing the noise in the image, increasing the sharpness [54]. After these image enhancements, the DCT coefficients, $c(k, n)$, described in Equation (2.3), are calculated based on the size of the considered image and by following Equation (2.4), the DCT matrix is calculated. As already discussed in Section 2.2.1, the ideal coefficients of this matrix to be extracted are those correspondent to the lower frequencies of the image, since those represent the most perceptual changes of the output. These coefficients are located in the top-left corner of the matrix and so a Zig-zag scanning of the matrix is done to select the $C_i$ coefficients to retrieve the hash vector, i.e. the key resultant from the image DCT analysis. Note that the number of coefficients retrieved from the DCT matrix is the bit-size of the key extracted and will take an important role throughout this entire work.

After the completion of the image treatment procedure, which can be resumed to the keys extracted from both the database and the image to be authenticated inputs, it is possible to correlate these results to evaluate the performance of the PUF system and determining the characteristics for the authentication process. In the correlation section of the algorithm, an intra-HD and inter-HD analysis was carried out with a sufficiently large database inputs. These calculations of the intra-HD and inter-HD quantities can be used to map all the hamming distances resultant from the images available and can be used to calculate the Uniqueness of the PUF devices, as stated

in Equation (2.9). Most importantly, these statistical analysis of multiple images of the PUF devices serves the purpose of determining the decision threshold used in the authentication process which will determine the maximum hamming distance that an image can have, while compared to the database, to be successfully authenticated. Lastly, by considering the intra-HD and inter-HD data taken, the PoE, considered in Equation (2.8), can be calculated to determine the efficiency and fallibility of the authentication process.

# CHAPTER 4

# Experimental Results

## 4.1 PUF Characterization

As previously stated, the three types of optical PUF tokens used in this characterization were the tracing paper, p-PUF, the plastic optical fiber, f-PUF, and the organic-inorganic hybrid, m-PUF. In Figure 4.1, the typical photos of a laser induced speckle can be seen with its respective RoI embedded in the physical target for each of the PUF tokens.

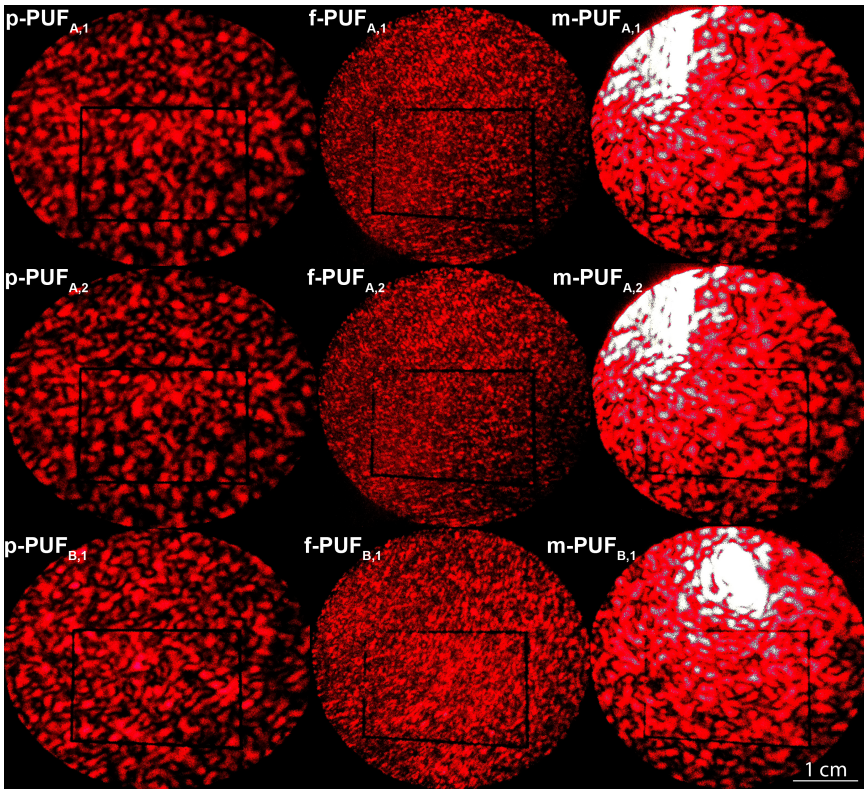


Figure 4.1: Photography of three speckle patterns produced by the samples p-PUF$_{A,B}$, f-PUF$_{A,B}$ and m-PUF$_{A,B}$, highlighting that between responses from the same sample there are a few differences as opposed to comparing the responses from different ones, which produce a completely new pattern. These images were taken using the custom camera parameters: brightness(60), ISO(800), saturation(30), sharpness(100), exposure compensation(25), contrast(100). Note that the darker rectangle present in the middle of the speckle pattern is the representation of the RoI that is embedded in the displaying target.

Figure 4.1 represents the speckle images taken to analyze the performance of the PUFs and the RoI was established in the physical target so that the process of digital image cropping becomes easier and a more precise task, while creating a common region between the different photos that will later be processed. As previously stated in section 2.2.1, this RoI was cropped from the images in Figure 4.1 and the DCT coefficients matching the size of the RoI were applied to the image input and the resulting DCT matrices for the different samples are displayed in Figure 4.2.

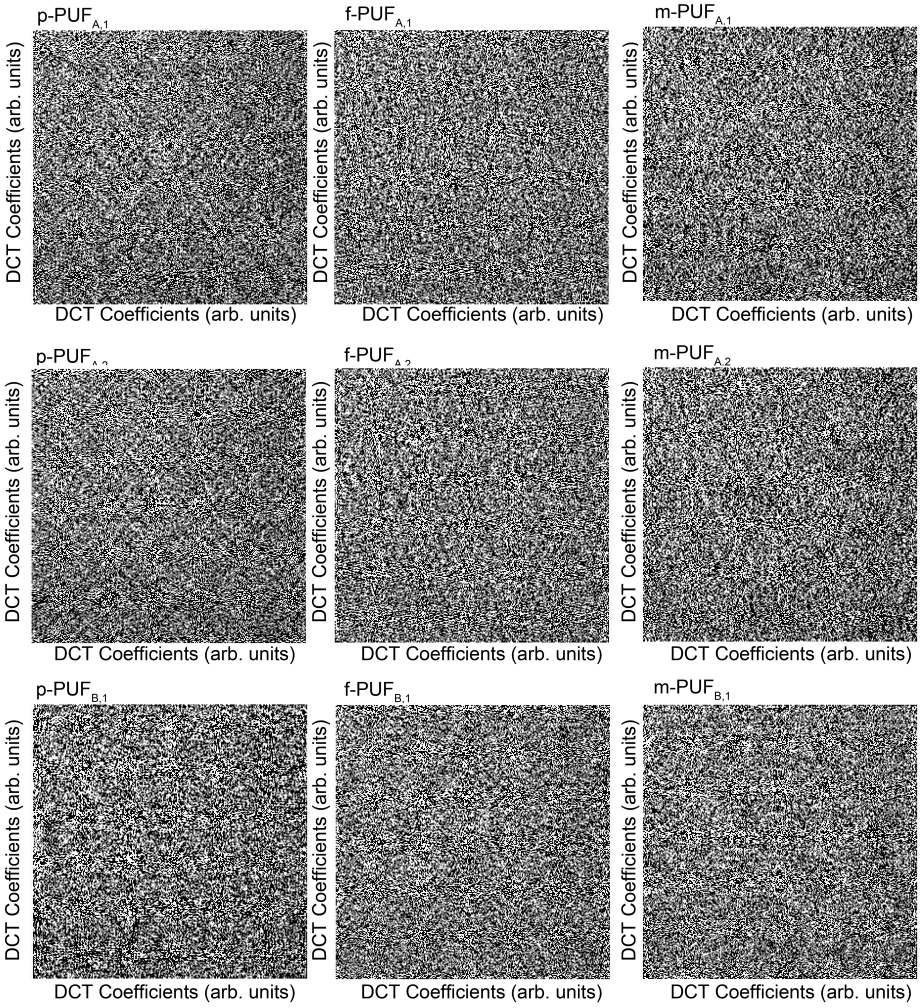


Figure 4.2: DCT matrix images using the RoI applied in Figure 4.1, for p-PUF, f-PUF and m-PUF. Note that, although the DCT matrices obtained between the same samples are different, the hash extraction is made only considering the top-left values of the matrices, which remain similar between samples. The black and white scale indicate values ranging from 0 to 1.

After constructing the DCT matrix image for that specific input, a 128-bit hash function was extracted. Note that the "DC term" described in Figure 2.5 was omitted in this 128-bit hash string to exclude the redundancy that this factor can have between the different PUF responses, creating a more unique hash vector for each input.

To evaluate the performance of the PUF device, a common approach is to compare the response of the same and different devices. The expectation between these comparisons is to have similar responses while using the same device and have completely different responses using a different device, while always stimulating the devices with the same challenge. The comparison metric used in this work is the already discussed normalized hamming distance, introduced in Equation (2.6). The hamming distances applied to images of the same and different devices are denoted intra-HD and inter-HD, respectively.

In Figure 4.3, these measurements are made considering the two p-PUF$_{A,B}$ devices used, where the intra-HD is measured by comparing all images from p-PUF$_A$ with themselves, combined with all the images of p-PUF$_B$ with themselves. The inter-HD was calculated by comparing all p-PUF$_A$ photos with all the p-PUF$_B$.

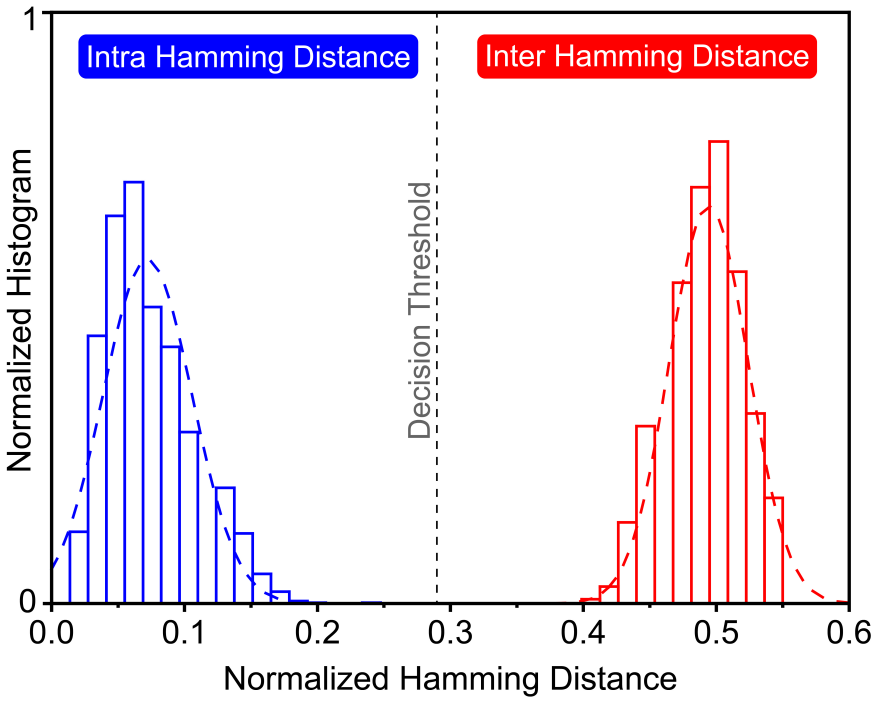


Figure 4.3: Histogram of the normalized hamming distance values retrieved by comparison of the 40 responses from p-PUF$_A$ and p-PUF$_B$, when retrieving a 128-bit hash function from the speckle response. An optimal decision threshold was calculated to distinguish between a successful authentication, hamming distance below the decision threshold, and a failed authentication, determined by having an hamming distance higher than the decision threshold.

The calculated hamming distance can be easily interpreted as the rate of errors while comparing the hash extracted from one photo to another. The normalization is made in such a way that an HD=0 represents an exactly perfect match between hashes, i.e. all the bits extracted are equal, while HD=1 shows that all the bits extracted are completely different. Furthermore, HD=0.5 corresponds to half the bits equal and half the bits unequal, between the hashes. As a consequence of these limits, an optimal

decision threshold was established to decide whether the hashes are extracted from the same device or from a different one, and, therefore, the commonly used boundary is described in Equation (2.7), which is the threshold level that minimizes the PoE, according to a "maximum likelihood" criteria. The employment of this decision threshold leads to two assignments: hamming distance values that are below the threshold are authenticated and higher hamming distances are not authenticated.

Figure 4.4 reflects and aid visual interpretation of some key results obtained using the normalized hamming distance metric applied to the 40 images acquired for each PUF sample, in the same conditions.

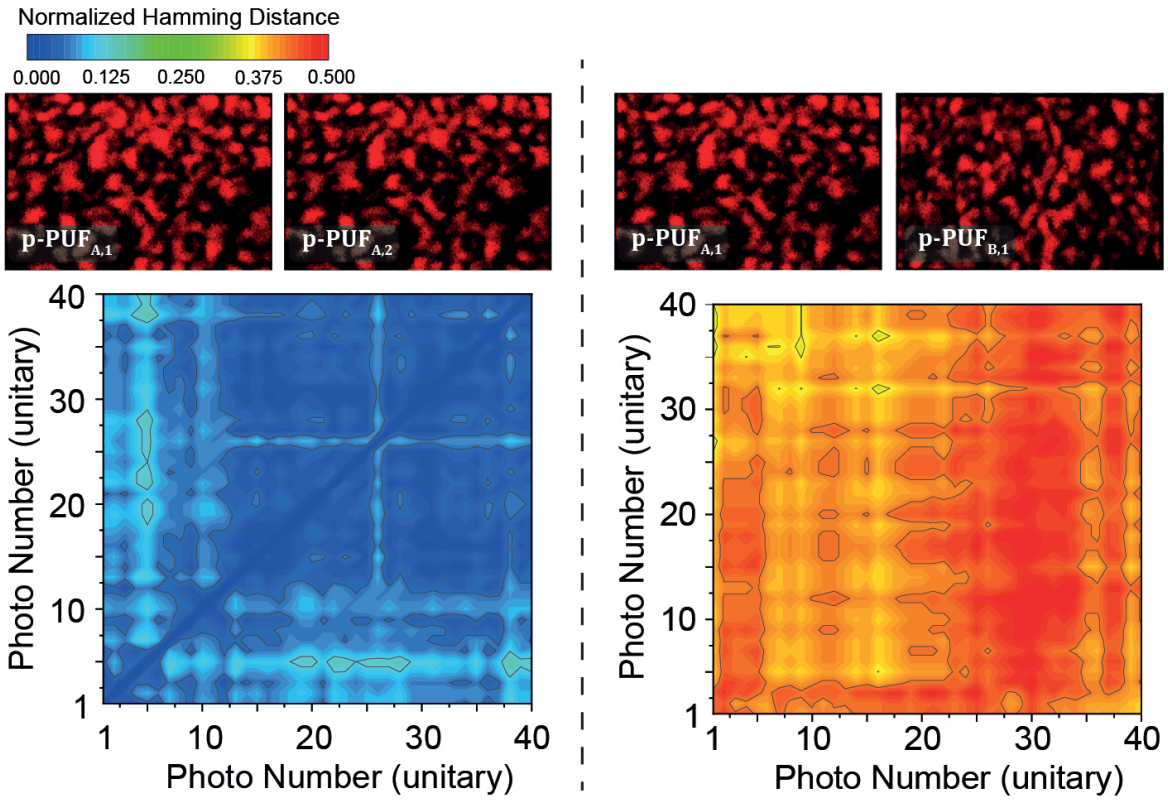


Figure 4.4: Mapping of the normalized hamming distances with sample speckle images for comparison. On the left, the p-PUF$_{A,1}$ is compared to p-PUF$_{A,2}$ which yields low hamming distance values since the speckles came from the same token. On the right, two different tokens are compared in terms of their speckle responses, when facing the same challenge, yielding higher hamming distance values across all the photos analysed.

When comparing input images of p-PUF$_{A,1}$, meaning the first image of 40 from sample A, and p-PUF$_{A,2}$, their responses, at bare sight, are identical and a few minor differences could be spotted. Accordingly, by yielding similar speckle patterns, the calculated normalized hamming distances reveal that the responses are correlated, i.e. the objects are correlated, which intrinsically means that the devices are the same if the

considerations described in Chapter 2.2 are valid. However, when comparing p-PUF$_{A,1}$ and p-PUF$_{B,1}$, the pattern speckles differ almost entirely, as expected, hence yielding a much higher hamming distance. Hence, by using the optimal threshold level, if p-PUF$_{A,1}$ is, for example, assumed to be the expected response stored in the database, a failure in the authentication of device p-PUF$_{B,1}$ will occur.

A similar analysis can be performed using a different token, in this case, the two small segments of a plastic optical fiber, denominated f-PUF$_A$ and f-PUF$_B$. The intra-HD and inter-HD values are displayed in Figure 4.5 and demonstrate similar results to those analysed in Figure 4.3.

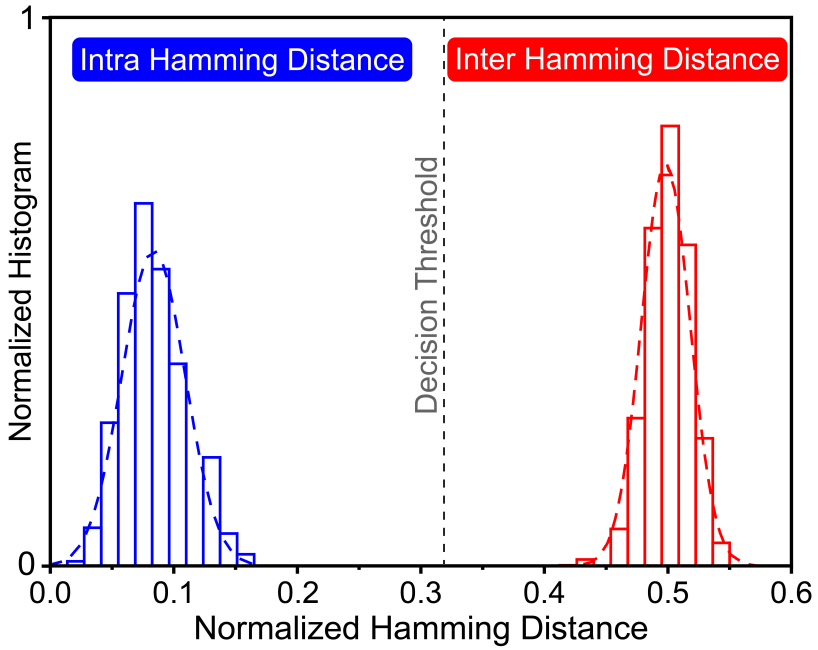


Figure 4.5: Histogram of the normalized hamming distance values retrieved by comparison of the 40 responses from f-PUF$_A$ and f-PUF$_B$, when retrieving a 128-bit hash function from the speckle response. An optimal decision threshold was calculated to distinguish between a successful authentication, hamming distance below the decision threshold, and a failed authentication, determined by having an hamming distance higher than the decision threshold.

The f-PUF token results attained for the intra-HD and inter-HD appeared to be coherent to those found when analysing the speckles from the tokens p-PUF. Experimentally, the changes in appearance of the speckle were not significant between the two tokens, which facilitated the analysis of the results in terms of the computational efforts needed. Moreover, since the two tokens can display similar speckle patterns it was confirmed that, disregarding the nature of the token, the details of the experimental system were consistent throughout the analysis.

Similar to the intra-HD and inter-HD histograms, an hamming distance mapping can provide valuable information about characteristics underlying the PUF authentication process while visually representing all the data collected for each PUF device.

In Figure 4.6, such mapping is obtained by comparing a total of 150 responses (i.e. speckle photos).

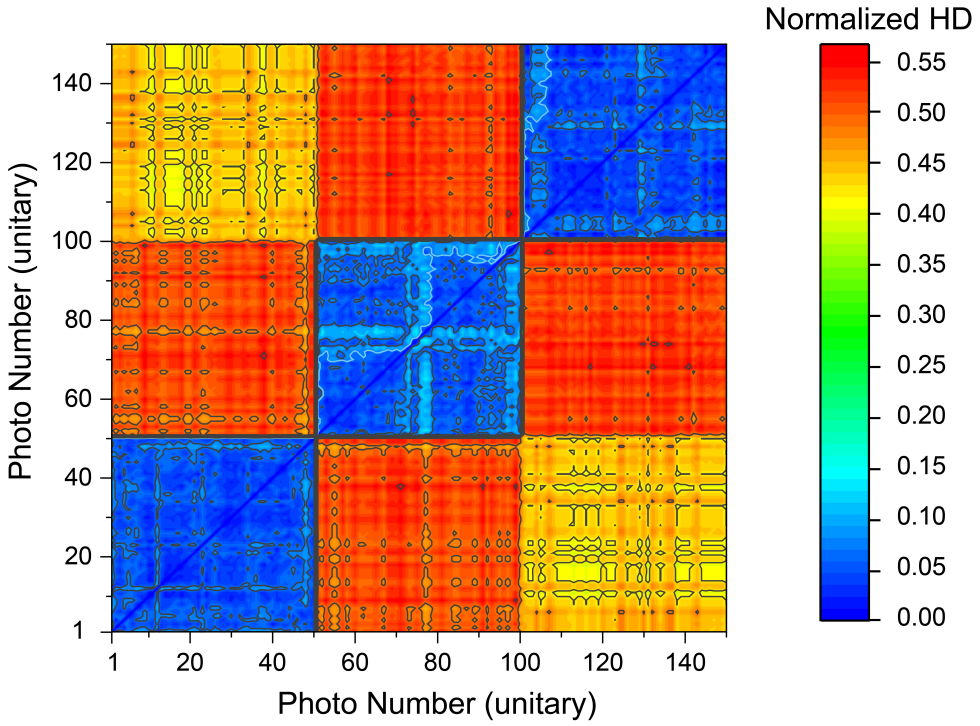


Figure 4.6: Mapping of the normalized hamming distances when comparing three different samples, A, B and C, of the f-PUF device. Note that the first 50 photos are referred to f-PUF$_A$, from 51-100 it is considered f-PUF$_B$, and, the last 50 photos, corresponds to the f-PUF$_C$ device.

Note that, in this case, three different samples are analysed: f-PUF$_A$, f-PUF$_B$ and f-PUF$_C$. The tokens f-PUF$_A$ and f-PUF$_B$ follow the rationalization applied until here: two different plastic optical fiber segments were cut and compared in different instances with the same laser challenge. However, f-PUF$_C$ is a different representation of f-PUF$_A$ since the object is the same, but rotated 180 degrees with respect to the axis perpendicular to the direction of propagation of the laser light, as described in Chapter 3. While the results appear to be consistent across the comparison of f-PUF$_A$ and f-PUF$_B$, i.e., images of the same device yields lower hamming distance and images between different devices presented much higher hamming distance, when f-PUF$_C$ is compared with f-PUF$_A$, the hamming distance lowers to about 0.40<HD<0.45. In fact, the device is the same, however, by changing its position relatively to the laser beam, the speckle pattern formed by the light dispersion will suffer alterations, increasing considerably the hamming distance calculated. The reasoning behind this analysis was to test if the placement of the token was impactful in the authentication process of the PUFs. The results attained considering f-PUF$_A$ and f-PUF$_C$ concluded that, if device A is stored in a database, then device C would not be authenticated based on

the optimal threshold value, despite the speckle images were, in fact, taken from the same device. Although the normalized hamming distance is lower comparing A-C than when comparing A-B, it is not significantly lower to pass the authentication process, hence, pointing that a careful positioning of the tokens has to be made in order to authenticate the device.

The last token used in speckle based PUF devices studied in this work is the monolith shaped device, with only one sample, named m-PUF, but with two different representations, m-PUF$_A$ and m-PUF$_B$, for different surfaces of the monolith, as described in Figure 3.2. In Figure 4.7, the typical intra-HD and inter-HD histogram can be seen and, as usual, the optimal decision threshold was calculated in order to determine the authentication success rate.

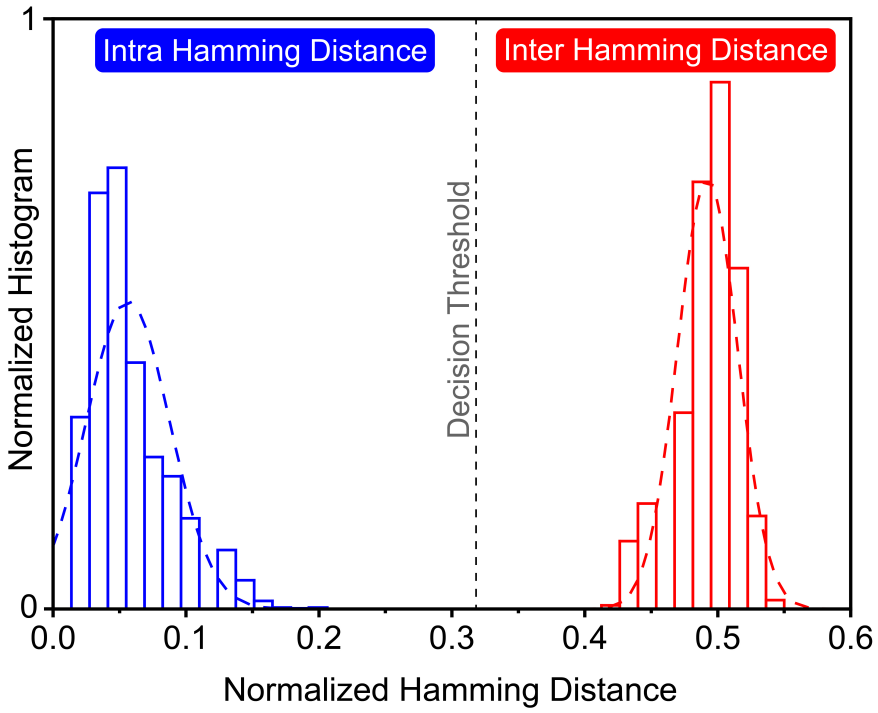


Figure 4.7: Histogram of the normalized hamming distance values retrieved by comparison of the 40 responses from m-PUF$_A$ and m-PUF$_B$, when retrieving a 128-bit hash function from the speckle response. An optimal decision threshold was calculated to distinguish between a successful authentication, hamming distance below the decision threshold, and a failed authentication, determined by having an hamming distance higher than the decision threshold.

Similar to the device p-PUF and f-PUF, m-PUF also presented a well-defined gaussian distribution both in the intra-HD and inter-HD configurations. Also in this analysis, an optimal decision threshold was defined for this token and will be used throughout the rest of the work, for security and authentication purposes. Additionally, it is important to mention that for the characterization of m-PUF token, a 128-bit hash string was retrieved from the speckle images that were generated by sample A and B. However, in

the case of this token, the different samples are designated by the same device, which can change its correspondent analysis. Despite this factor, the analysis made earlier with f-PUF$_{\mathrm{A}}$ and f-PUF$_{\mathrm{C}}$, revealed that the same device can produce speckle patterns distinct enough to perform secure authentication, which will later be discussed.

To summarize the results obtained with the three different token devices, p-PUF, f-PUF and m-PUF, one has to determine the key characteristics of the normalized hamming distance analysis. These parameters are the mean value, $\mu$, and standard deviation, $\sigma$, of the gaussian distributions that identify the intra-HD and inter-HD and the resultant optimal decision threshold, $d_{\mathrm{opt}}$ calculated. In Table 4.1, those values are displayed and will be later used for the security analysis of the optical PUF devices. The values for the False Negative Rate (FNR), also denominated as the probability P(0|1), and the FPR, which is also the name for the probability P(1|0), are also presented in Table 4.1.

Table 4.1: Summary of the intra-HD and inter-HD parameters considered in the gaussian distribution fitting for each type of PUF device, regarding their hamming distances.

| | $\mu_{\text{intra-HD}}$ | $\mu_{\text{inter-HD}}$ | $\sigma_{\text{intra-HD}}$ | $\sigma_{\text{inter-HD}}$ | $d_{\mathrm{opt}}$ | FNR | FPR |
|---|---|---|---|---|---|---|---|
| p-PUF | 0.072 | 0.494 | 0.034 | 0.030 | 0.296 | $10^{-11}$ | $10^{-11}$ |
| f-PUF | 0.084 | 0.498 | 0.026 | 0.020 | 0.318 | $10^{-19}$ | $10^{-19}$ |
| m-PUF | 0.056 | 0.492 | 0.031 | 0.022 | 0.310 | $10^{-17}$ | $10^{-16}$ |

Attending to Table 4.1, it is clear that all the PUF tokens performed equally regarding $\mu$, $\sigma$ and $d_{\mathrm{opt}}$. Despite these similarities, minor changes in these values yielded very different FNRs and FPRs due to their high susceptibility, since the values for P(0|1) and P(1|0) are so low. This fact does not pose any direct disadvantage to any token performance but does provide valuable information about the performance of each one. In this case, the best performing token was the f-PUF, followed by m-PUF and then p-PUF, which achieved FNR and FPR scores of $10^{-11}$, which are the lowest values across all the tokens studied.

## 4.2 Authentication and Security Performance

In this section, the security aspects of the PUF tokens (p-PUF, f-PUF and m-PUF) will be detailed. Most of these results can be achieved by using the data described in Table 4.1, combined with the formulation applied on Equations (2.7) and (2.8), for the optimal threshold level and the PoE, respectively. By doing so, it is possible to calculate the PoE in the authentication process across all the PUF devices queried. In addition to that, since the PoE is a quantitative metric of the performance and fallibility of the system, it was used to ascertain the influence that the size of the hash vector has in the authentication and performance of the system. The method used to perform this study was to retrieve the hash strings of each of the responses from the PUF tokens, with different numbers of extracted bits per each trial. In each of those

cases, the optimal decision threshold was determined and the areas of the overlapping curves were calculated, yielding the PoE value, as explained in Equation (2.8). The PoE results regarding the variable number of extracted bits can be seen in Figure 4.8.

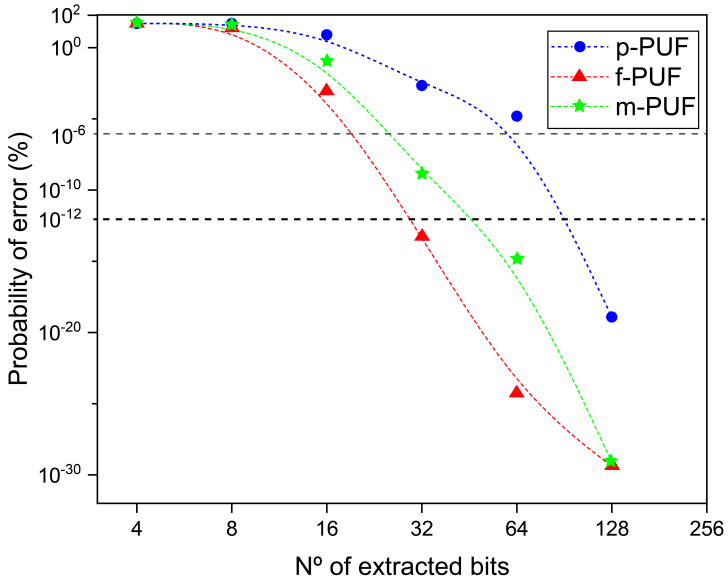


Figure 4.8: Representation of the PoE changes when using a different number of bits extracted from the DCT matrix image. Note that the level $10^{-6}$ is the standard PoE limit without any ECC algorithm and that $10^{-12}$ is the PoE limit for detection [55]. Note that the lines are visual guides for the trends observed.

In this case, the number of extracted bits represents the length of the hash vector and the errors are the mismatch between the bits retrieved and the bits stored in the database. The standard PoE limit for these applications, and without any ECC algorithm, is below $10^{-6}$, while the PoE limit for detection is usually considered to be $10^{-12}$ [55].

As it can be seen in Figure 4.8, the f-PUF and m-PUF devices studied can perform below the standard limit of PoE$< 10^{-6}$ when the bit-string size is higher than 16 bits, while the p-PUF can achieve this threshold using 64 bits. As for the limit of detection of PoE$< 10^{-12}$, the f-PUF can operate at 32 bits, while m-PUF needs 64 bits and p-PUF 128 bits. Based on these results, in terms of fallibility of the PUF authentication decision process, the f-PUF device performs the best and p-PUF performs the worst. However, the difference in implementation complexity and versatility could play an important role in the decision between which token to adopt in PUF-based cryptographic system. Since all the devices were able to perform below the thresholds defined for optimal cryptographic key transmission, all of the tokens are eligible to be used. It is also important to note that, although the bit stream sizes appear to be small, they are sufficient to achieve efficient key transmissions and the 128-bit size hash vector is often used in many cryptographic studies [17, 55].

All the results discussed up to this point showed a possibility, across all tokens

used, of having an authentication protocol based on the speckle images generated by the PUFs, stored in a database for posterior comparison. To summarize these findings, in Figure 4.9, the *uniqueness* is presented for each token, based on Equation (2.9).

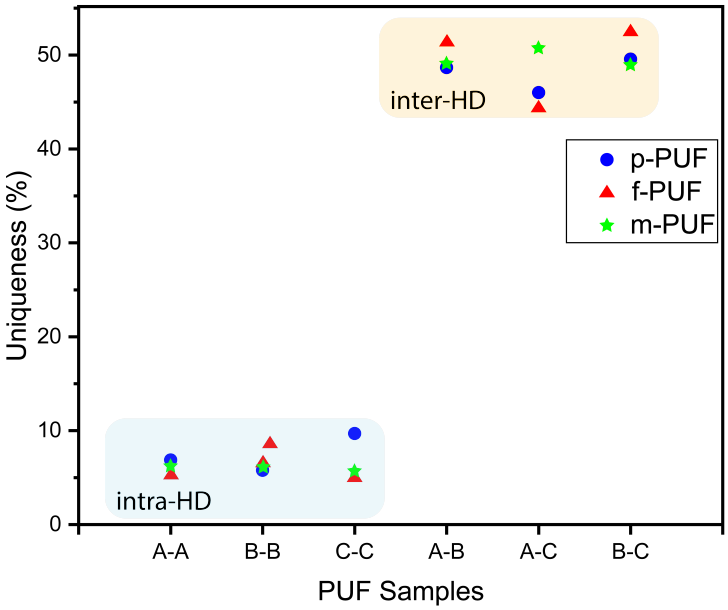


Figure 4.9: Representation of the *uniqueness* for the three PUF tokens studied, considering three samples for each of them. Note that samples A and B were designated considering different devices, except in the m-PUF case, as previously discussed. The sample C for each of the PUF tokens was a result of a positional transformation of sample A, thus yielding slightly less *uniqueness* values when comparing A and C.

Across all devices, the speckle image authentication, when compared to the key stored, present a *uniqueness* below 10% which indicates that the device being evaluated is valid to be authenticated. However, when compared to images from different devices, the *uniqueness* increases to about 50%, concluding that the user is not authenticated. Evaluating the different samples (A, B and C) from each device, it is possible to note that the *uniqueness* values calculated considering the same token sample, referring to A-A, B-B and C-C in Figure 4.9, are low and comparable between the devices, with only small experimental deviations. While comparing devices A-B and B-C, the *uniqueness* values are also comparable and high enough to assume that the devices are different. However, when comparing samples A and C, namely in p-PUF and f-PUF devices, the *uniqueness* value lowers slightly which is a reflection on the similarity that the two samples have, due to being designated from the same device. Nevertheless, while comparing devices A and C in the m-PUF token, the *uniqueness* value appear to not change, which suggests that this token possesses another intrinsic dynamic that its highly sensitive to the positioning of the token.

Although these results showed a promising implementation of these devices, a malicious attempt to decrypt the key stored can be made by using "brute-force" methods of

retrieving the correct key. By purely guessing the binary key retrieved from an image, the probability of a successful authentication can be interpreted as:

$$P_a = 2^{-M}, \tag{4.1}$$

where $M$ is the number of bits used per key. Evidently, as $M$ increases, the probability of randomly guessing the key stored decreases and, by only using 256 bits, the chances of getting a successful authentication are 1 in $10^{79}$.

However, the interpretation is only valid to an equiprobable number of ones and zeros in each key, which is essentially testing if the key generated per each device is a truly random number. To characterize the bit strings as such, there are several statistical tests that may be employed to investigate the degree of randomness of a binary sequence and to check the generated bit string for specific weaknesses to targeted attacks. The obtained sequences passed the standard NIST Randomness Tests suites [56] and the results of the most commonly used tests are shown in Figure 4.10. The NIST tests were applied individually to 360 binary sequences, combining the hash strings retrieved from the p-PUFs, f-PUFs and m-PUFs.

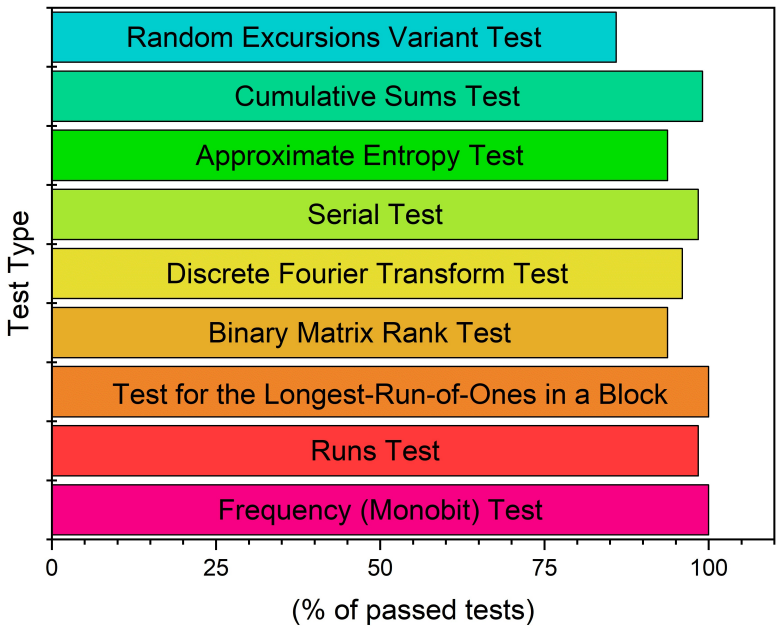


Figure 4.10: NIST statistical tests scores describing the approval rates for a total of 360 binary sequences with 128 bits each, retrieved from the multimedia files recorded using p-PUF, f-PUF and m-PUF [56].

The results attained, with exception of the "Random Excursions Variant Test", showed a test acceptance rate higher than 90%, indicating that the keys extracted from these devices can be considered random. Combining the random nature of these keys with the propriety that these devices are physical one-way functions, the possibility of hacking these cryptographic systems is highly diminished.

# CHAPTER 5

## Conclusions

In this work, it was demonstrated the photonic implementation and characterization of three different low cost PUF tokens: tracing paper, plastic optical fiber and organic-inorganic hybrid. This implementation consisted in both the production and the recording of speckle patterns which were originated due to the laser illumination of the tokens. One of the most important steps to achieve these results was setting the parameters of the camera. Although no quantitative approach was considered, several images in different scenarios were recorded and the algorithm for PUF authentication was applied, ensuring that the best results were discussed in this work.

The normalized hamming distance mapping and histogram results presented valuable information about the authentication parameters to be used in PUF authentication, concerning the three tokens used, namely, the optimal decision threshold for authentication success. Particularly, in the hamming distance mappings, an overview of all the hamming distances is presented, which clearly shows the differences between an authentication of the same or distinct devices.

Considering the "uniqueness" results, the intra-HD and inter-HD values suggests very strongly that the PUFs implemented are highly influenced by their positioning. This result, along with the fact that the objective is to reduce the complexity of the system, sets precedents for the upcoming work, since the position of the PUF has to be carefully considered. On the other hand, the sensitivity that PUFs have shown concerning the relative positioning in regards to the rest of the system, revealed to be positive because it is possible to conclude that this system is highly secured and robust and that the minimal change in the PUF, immediately yields a failure in authentication, which decreases the possibility of cloning this system by a third party.

The PUF authentication system was tested regarding the security. In the authentication process, these tests were conducted using the PoE metric that was established considering the parameters calculated in prior hamming distance tests. The PoE was calculated for each token, accounting the number of bits extracted in each trial. All the tokens produced a PoE result below $10^{-12}$, detection limit, with a 128-bit encryption system, with f-PUF yielding the best results and p-PUF the worst. Moreover, the NIST statistical tests for random number generators were conducted to evaluate the randomness of the key extracted from the speckle images. The vast majority of the tests scored over 90% of acceptance rate which indicates a very good resilience against targeted attacks from unwanted parties.

In terms of the computational complexity and efficiency of the PUF authentication process, the main difficulties while performing this work were: the determination of

the RoI and the speckle image storage. The determination of the RoI, although it was established in the physical target, subjective factors, such as the boundaries of such region and the orientation of the region, i.e. assuring that the camera is positioned correctly in relation to the target, was challenging. The image storage also presented a drawback since this work was maintained manual to reduce the complexity of the system but increased the time spent in preparing the images for software analysis which requires an optimization process in the future.

Concerning the portability and versatility of this PUF system to be applied in a realistic scenario, the main obstacle is the usage of the beam expander which was integrated to obtained clearer speckle images. To reduce the complexity of the system, one can remove this component at the expense of an image quality reduction. However, as previously stated, since the system obtained high performance results across all the PUF tokens, it is possible to compromise this performance in order to achieve a more portable and compact system.

Overall, the PUF implementation is considered valid and promising due to the high security of the system and the high scores in the authentication process, while using tokens of low complexity, such as p-PUF and f-PUF, and also tokens with higher versatility and complexity such as the m-PUF. Furthermore the system is considered to be user-friendly in the sense that can be previously programmed to be used in many security applications.

## 5.1 Future Work

During this work, a type-II DCT analysis of the images were considered. Although this was the only method for image-based hash extraction used in this work, it is acknowledged that there are many more algorithms capable of performing this technique and were briefly explained in Chapter 1.3. Considering different algorithms for hash extraction would be beneficial to increase the performance and security of this PUF system and, thus, a more in-depth study of this algorithms is advised.

As previously stated, the intra-HD and inter-HD levels were highly distinguishable using these methods, which suggests that the complexity of the system can be decreased in order to increase the portability and versatility of the system, without compromising neither the security or the fallibility. The removal of the beam expander and the substitution of the laser source for a smaller one would be beneficial to achieve a more robust system and with a higher compatibility in a more compact environment. However, the tests discussed in this dissertation, or other equivalents, need to be applied to ensure that the authentication performance and security remains elevated.

Although, in this work, no ECC algorithms were implemented, they are widely used in the cryptographic and communication areas to enhance the performance of the hashing process without physically changing the system and without additional hardware costs. If ECC protocols were implemented in this context and provided an increase in the performance of the system, once again, this gain would provide

the possibility of having a cost-efficient trade-off, for example, by removing the beam expander or decreasing the required quality of the camera.

Another important test to be considered in the future application of the PUF tokens is time-resolved hamming distance within the same device, i.e., comparing the initial PUF speckle pattern with the following patterns obtained in other instances. Although the response durability and consistency of these tokens can be bypassed by regularly updating the database with new images, it is desirable that, to some extent, this proprieties remain stable for a longer period of time. The short-term analysis performed in this work showed no noticeable degradability after the average measurement time of 3-4 hours, but no extensive tests were performed.

Moreover, PUF positioning and mechanical stress studies should also be considered to identify the effect that these proprieties have in the speckle patterns and how that can be mitigated or even used as an advantage to strengthen the authentication process.

Ultimately, one of the most important features that could be introduced in this system is the ability of doing smartphone-based authentication. To achieve that, image correction algorithms would need to be applied to select the correspondent speckle RoI to be authenticated. Since the results attained in this work revealed a high-performing PUF authentication system, the downgrading of the imaging system is therefore compensated, which provides a more mobile and user-friendly experience. The objective would be to have a server with a database of stored speckle images that would be used to perform remote access authentication. Once the user uploads the respective speckle response recorded, the algorithm would be applied to, firstly, correct the image and, then, to apply the necessary steps to authenticate the user.

Lastly, the implementation of tokens such as the m-PUF would be very beneficial in some applications. As previously stated, these materials can be processed in many formats which grants them the advantage of being integrated in several devices for authentication purposes. Possible implementations of these materials would be to deposit them in a certain product, for product tagging intents, or to incorporate them in a physical device, such as a card, to enable physical access to a secure location or deposit. The potential of these devices to be incorporated in such applications, allied with smartphone-based authentication protocols, could be promising in cryptographic systems with remote key storage.

# Bibliography


[1] K. P. Satamraju and B. Malarkodi. A PUF-based mutual authentication protocol for internet of things. In *2020 5th International Conference on Computing, Communication and Security (ICCCS)*, pages 1–6.

[2] Miguel Ángel Prada-Delgado, Iluminada Baturone, Gero Dittmann, Jens Jelitto, and Andreas Kind. PUF-derived IoT identities in a zero-knowledge protocol for blockchain. *Internet of Things*, 9:100057, 2020.

[3] R. P. Singh, M. Javaid, A. Haleem, and R. Suman. Internet of things (iot.

[4] Ana R. Bastos, Guanpeng Lyu, Tiago Silvério, Paulo S. André, Rachel C. Evans, and Rute A.S. Ferreira. Flexible blue-light fiber amplifiers to improve signal coverage in advanced lighting communication systems. *Cell Reports Physical Science*, 1(4):100041, 2020.

[5] Tiago Silvério, Gonçalo Figueiredo, Paulo S. André, and Rute A.S. Ferreira. Privacy increase in VLC system based on hyperchaotic map. In *2021 Telecoms Conference (ConfTELE)*, pages 1–4, 2021.

[6] Fortune Business Insights. Internet of things market size, growth: IoT industry report [2020-2027], Jul 2020.

[7] International Data Corporation. Business models for the long-term storage of internet of things use case data, Jul 2020. Online. https://www.idc.com/getdoc.jsp?containerId=AP45984120/ (Accessed 2021-05-15).

[8] Netscout. Netscout threat intelligence report - findings from the first half of 2018, Jul 2018. Online. https://www.netscout.com/threatreport/ (Accessed 2021-05-16).

[9] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, N. Md Nainar, A. S. M.and Akim, and M. Imran. Deep learning and big data technologies for IoT security. *Computer Communications*, 151:495–517, 2020.

[10] Kenneth Kimani, Vitalice Oduol, and Kibet Langat. Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25:36–49, 2019.

[11] Alison F. Smith and Sara E. Skrabalak. Metal nanomaterials for optical anti-counterfeit labels. *Journal of Materials Chemistry C*, 5(13):3207–3215, 2017.

[12] Global brand counterfeiting report 2018-2020 - researchandmarkets.com, May 2018.

[13] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T.s Nikas, and D. Syvridis. Physical unclonable function based on a multi-mode optical waveguide. *Scientific Reports*, 8(1):9653, 2018.

[14] C. Chaintoutis, M. Akriotou, C. Mesaritakis, I. Komnios, D. Karamitros, A. Fragkos, and D. Syvridis. Optical PUFs as physical root of trust for blockchain-driven applications. *IET Software*, 13, 12 2018.

[15] Miguel R. Carro-Temboury, Riikka Arppe, Tom Vosch, and Thomas Just Sørensen. An optical authentication system based on imaging of excitation-selected lanthanide luminescence. 4(1):e1701384, 2018.

[16] Basel Halak. Physically unclonable functions : From basic design principles to advanced hardware security applications. 2018.

[17] S. Urban A. Weiershäuser E. Dinter B. Forster C. Jirauschek U. Rührmair, C. Hilgers. Optical PUFs reloaded. Eprint.Iacr.Org, 2013. https://doi.org/10.1109/sp.2013.27.

[18] Tao Yang, Chai Wah Wu, and L.O. Chua. Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 44(5):469–472, 1997.

[19] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, CCS '02, page 148–160, NY, USA, 2002.

[20] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026, 2002.

[21] E.R. Berlekamp. The technology of error-correcting codes. *Proceedings of the IEEE*, 68(5):564–593, 1980.

[22] Albert Einstein. Zur Quantentheorie der Strahlung. *Phys. Z.*, 18:121–128, 1917.

[23] J. P. Gordon, H. J. Zeiger, and C. H. Townes. The maser-new type of microwave amplifier, frequency standard, and spectrometer. *Phys. Rev.*, 99:1264–1274, Aug 1955.

[24] T. H. Maiman. Stimulated optical radiation in ruby. *Nature*, 187(4736):493–494, 1960.

[25] Walter Koechner. *Solid state laser engineering / Walter Koechner.* Springer series in optical sciences ; v. 1. Springer-Verlag, New York, 1976.

[26] Thorlabs. *HNLS008R - Self-Contained HeNe Laser System.* Thorlabs, USA, March 2015. [Online].

[27] J. Wilson and J. F. B. Hawkes. *Optoelectronics : an introduction / J. Wilson, J.F.B. Hawkes.* Prentice-Hall international series in optoelectronics. Prentice-Hall, Englewood Cliffs, N.J, second edition. edition, 1989.

[28] H. Haken. *Laser theory.* Springer-Verlag, 1984.

[29] Emil Wolf. *Introduction to the theory of coherence and polarization of light.* Cambridge University Press, Cambridge, 2007.

[30] Yuanbo Deng and Daping Chu. Coherence properties of different light sources and their effect on the image sharpness and speckle of holographic displays. *Scientific Reports*, 7(1):5893, 2017.

[31] A. El Gamal and H. Eltoukhy. CMOS image sensors. *IEEE Circuits and Devices Magazine*, 21(3):6–20, 2005.

[32] B. S. Carlson. Comparison of modern CCD and CMOS image sensor technologies and systems for low resolution imaging. In *SENSORS, 2002 IEEE*, volume 1, pages 171–176 vol.1.

[33] Pierre Magnan. Detection of visible photons in CCD and CMOS: A comparative view. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 504(1):199–212, 2003.

[34] M. Garcia-Bosque, G. Díez-Señorans, C. Sánchez-Azqueta, and S. Celma. Introduction to physically unclonable fuctions: Properties and applications. In *2020 European Conference on Circuit Theory and Design (ECCTD)*, pages 1–4.

[35] S. Dolev, L. Krzywiecki, N. Panwar, and M. Segal. Optical PUF for non forwardable vehicle authentication. In *2015 IEEE 14th International Symposium on Network Computing and Applications*, pages 204–207.

[36] Auguste Kerckhoffs. Desiderata de la cryptographie militaire. *Journal des sciences militaires*, IX(13):5–83, 1883.

[37] F. Afghah S. Zeadally A. Shamsoshoara, A. Korenda. A survey on physical unclonable function (PUF)-based security solutions for internet of things. *Computer Networks*, 183:107593, 2020.

[38] O. Günlü and O. İşcan. DCT based ring oscillator physical unclonable functions. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 8198–8201.

[39] Zeng Jie. A novel block-DCT and PCA based image perceptual hashing algorithm. *International Journal of Computer Science Issues*, 10, 2013.

[40] F. Ahmed and M. Y. Siyal. A secure and robust DCT-based hashing scheme for image authentication. In *2006 10th IEEE Singapore International Conference on Communication Systems*, pages 1–6.

[41] O. Günlü, O. İşcan, and G. Kramer. Reliable secret key generation from physical unclonable functions under varying environmental conditions. In *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6.

[42] I. Shin and H. W. Park. Adaptive up-sampling method using DCT for spatial scalability of scalable video coding. *IEEE Transactions on Circuits and Systems for Video Technology*, 19(2):206–214, 2009.

[43] Lin Ching-Yung and Chang Shih-Fu. A robust image authentication method distinguishing JPEG compression from malicious manipulation. *IEEE Transactions on Circuits and Systems for Video Technology*, 11(2):153–168, 2001.

[44] Keith Jack. *Chapter 5 - Digital Video Processing*, pages 125–150. Newnes, Burlington, 2008.

[45] Sandeep R and Prabin Bora. *Perceptual video hashing based on the Achlioptas's random projections*. 2013.

[46] C. Zauner. Implementation and benchmarking of perceptual image hash functions.

[47] A. Swaminathan, Mao Yinian, and Wu Min. Robust and secure image hashing. *IEEE Transactions on Information Forensics and Security*, 1(2):215–230, 2006.

[48] João F. C. B. Ramalho, L. C. F. António, S. F. H. Correia, L. S. Fu, A. S. Pinho, C. D. S. Brites, L. D. Carlos, P. S. André, and R. A. S. Ferreira. [invited] luminescent QR codes for smart labelling and sensing. *Optics  Laser Technology*, 101:304–311, 2018.

[49] S. Sankaran, S. Shivshankar, and K. Nimmy. Lhpuf: Lightweight hybrid PUF for enhanced security in internet of things. In *2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, pages 275–278.

[50] Sandra F. H. Correia, Patrícia P. Lima, Paulo S. André, Maria Rute Sá Ferreira, and Luís António Dias Carlos. High-efficiency luminescent solar concentrators for flexible waveguiding photovoltaics. *Solar Energy Materials and Solar Cells*, 138:51–57, 2015.

[51] João F. C. B. Ramalho, Sandra F. H. Correia, Lianshe Fu, Lília M. S. Dias, Pedro Adão, Paulo Mateus, Rute A. S. Ferreira, and Paulo S. André. Super modules-based active qr codes for smart trackability and IoT: a responsive-banknotes case study. *npj Flexible Electronics*, 4(1):11, 2020.

[52] Ahmad Reza Bagheri and Nahal Aramesh. Towards the room-temperature synthesis of covalent organic frameworks: a mini-review. *Journal of Materials Science*, 56(2):1116–1132, 2021.

[53] Camera module - Raspberry Pi documentation. Online. (Accessed 2021-05-17) https://www.raspberrypi.org/documentation/hardware/camera.

[54] Orhan Akbulut, Oguzhan Urhan, Sarp Erturk, and Tae-Gyu Chang. One-dimensional processing for efficient optimal post-process/in-loop filtering in video coding. *IEEE Transactions on Consumer Electronics*, 54(3):1346–1354, 2008.

[55] I. Haider, M. Höberl, and B. Rinner. Trusted sensors for participatory sensing and IoT applications based on physically unclonable functions. In *Proceedings 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, page 14–21.

[56] J. Nechvatal M. Smid E. Barker S. Leigh M. Levenson M. Vangel D. Banks A. Heckert J. Dray S. Vo A. Rukhin, J. Soto. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *NIST Publication 800-22rev1*, 2008.